Igiena Digitală:

Handbook pentru Startup-uri

BDA

mathemagenesis

MUĞLA SITKI KOÇMAN ÜNİVERSİTESİ

eLearning software

EduVibes

WITTENBORG University of Applied Sciences

Co-funded by the European Union

GOOD START

Good Digital Hygiene for Startups

Nr. proiect: 2022-1-LV01-KA220-VET-000086725 | Titlu proiect: „Good Digital Hygiene for Startups”

Cuprins

Modulul 1 – Igiena Digitală: definiții și termeni

Unitatea 1 – Concepte de referință pentru Igiena Digitală

În condițiile evoluției rapide a contextului antreprenoriatului digital, startup-urile se confruntă cu o multitudine de provocări generate atât de competiția acerbă, cât și de resursele limitate. Ținând cont de aceste provocări, asigurarea practicării unei Igiene Digitale puternice este esențială pentru o creștere sustenabilă și succesul startup-urilor.

Conceptul de Igienă Digitală se bazează pe mai multe cadre de referință teoretice și principii din diverse domenii, inclusiv securitatea cibernetică, managementul informațiilor și comportamentul organizațional. Există câteva teorii-cheie pe care se bazează conceptul de Igienă Digitală:

1. Teoria Securității Cibernetice (Cybersecurity)

Teoria securității cibernetice reunește principii și modele variate ce urmăresc înțelegerea și soluționarea amenințărilor și vulnerabilităților cibernetice. Triada CID (Confidențialitate, Integritate, Disponibilitate) reprezintă un concept fundamental pentru Teoria securității cibernetice, subliniind importanța protejării datelor împotriva accesului neautorizat (confidențialitate), asigurării acurateții și credibilității datelor (integritate) și menținerii accesului la date pentru utilizatorii autorizați (disponibilitate). Alte teorii ale securității cibernetice, precum modelul „Apărare în profunzime” (Defense-in-depth) și modelul „Zero Încredere” (Zero Trust), furnizează cadrele de referință pentru proiectarea și implementarea unor strategii robuste de Securitate cibernetică, pentru a reduce riscurile și a proteja împotriva atacurilor cibernetice.

2. Teoria managementului informației

Teoria managementului informației se concentrează pe administrarea eficientă a resurselor informaționale din organizații. Modelul „Administrarea ciclului de viață a Informației” este un cadru de referință teoretic care descrie etapele prin care trece informația de la creare la eliminare, subliniind importanța gestionării informației de-a lungul ciclului de viață pentru a asigura confidențialitatea, integritatea și disponibilitatea. Principiile de guvernanță a datelor, de administrare a datelor și de gestionare a calității datelor sunt, de

asemenea, esențiale pentru teoria managementului informației, orientând modul în care organizațiile își pot administra și proteja eficient resursele informaționale.

3. Teoria factorului uman

Teoria factorului uman explorează rolul comportamentului uman, al cunoașterii și luării deciziilor în contextul securității cibernetice. Teoria Erorii Umane sugerează că eroarea umană contribuie semnificativ la incidentele cibernetice și la încălcarea securității datelor, subliniind importanța instruirii, conștientizării și capacității de utilizare în ceea ce privește reducerea riscurilor generate de greșeli umane. Teoria Comportamentului planificat (the Theory of Planned Behavior) și Modelul acceptării tehnologiei (the Technology Acceptance Model – TAM) sunt alte cadre conceptuale teoretice care explică cum atitudinile, credințele și percepțiile indivizilor le pot influența comportamentul în ceea ce privește adoptarea practicilor și tehnologiilor de securitate cibernetică.

4. Teoria comportamentului organizațional

Teoria comportamentului organizațional examinează modul în care indivizii, grupurile și structurile din organizații interacționează și influențează comportamentul. Structura tehnologie-organizație-mediu este un model teoretic care explică factorii care influențează adoptarea și implementarea tehnologiei informației în organizații, inclusiv factorii tehnologici, factorii organizaționali și factorii de mediu. Teoria difuzării inovațiilor, dezvoltată de Everett Rogers, explorează modul în care noile idei, tehnologii și practici se răspândesc în cadrul societăților și organizațiilor, oferind perspective asupra adoptării și difuzării practicilor de Igienă Digitală în cadrul startup-urilor și al altor contexte organizaționale.

5. Teoria conformității

Teoria conformității abordează factorii care influențează respectarea regulilor, reglementărilor și normelor de către indivizi și organizații. Teoria comportamentului planificat și teoria acțiunii motivate sunt modele teoretice care explică intenția indivizilor de a respecta regulile și reglementările bazate pe atitudinile lor, normele subiective și controlul comportamental perceput. Aceste teorii oferă perspective asupra modului în care startup-urile și organizațiile pot promova respectarea reglementărilor și standardelor de securitate cibernetică prin educație, formare, stimulente și mecanisme de aplicare.

Astfel, conceptul de igienă digitală integrează perspective și abordări multidisciplinare pentru a aborda provocările complexe ale securității cibernetice, managementului informațiilor, comportamentului uman și dinamicii organizaționale în cadrul startup-urilor și al altor organizații.

De asemenea, concepte suplimentare oferă o bază pentru înțelegerea și implementarea practicilor de igienă digitală în cadrul startup-urilor, asigurând protecția, integritatea și reziliența infrastructurii și operațiunilor lor digitale:

A) Securitatea cibernetică

Securitatea cibernetică reprezintă practica de protejare a sistemelor, rețelelor și datelor digitale împotriva accesului neautorizat, a atacurilor cibernetice și a încălcării datelor. Aceasta cuprinde diverse tehnologii, procese și practici menite să protejeze resursele digitale și să asigure confidențialitatea, integritatea și disponibilitatea informațiilor.

B) Confidențialitatea datelor

Confidențialitatea datelor se referă la protecția informațiilor personale și sensibile împotriva accesului, utilizării sau divulgării neautorizate. Aceasta implică respectarea reglementărilor și standardelor care reglementează colectarea, stocarea și prelucrarea datelor, cum ar fi GDPR, HIPAA sau CCPA, pentru a proteja dreptul persoanele la confidențialitate.

C) Managementul riscurilor

Managementul riscurilor implică identificarea, evaluarea și atenuarea riscurilor asociate cu operarea într-un mediu digital. Aceasta include implementarea controalelor și măsurilor pentru prevenirea, detectarea și răspunsul la potențialele amenințări și vulnerabilități care ar putea afecta operațiunile, reputația sau stabilitatea financiară a unui startup.

D) Cadre de conformitate și de reglementare

Respectarea reglementărilor și a standardelor din industrie este esențială pentru ca startup-urile să asigure activități legale și etice. Cadrele de reglementare, cum ar fi GDPR, HIPAA, PCI DSS sau SOX, oferă linii directoare și cerințe pentru protecția datelor, securitate și confidențialitate pe care startup-urile trebuie să le respecte pentru a evita repercusiunile legale și financiare.

E) Sisteme de management al securității informației (SMSI)

Cadrele conceptuale SMS**I**, cum ar fi ISO / IEC 27001, oferă o abordare sistematică pentru gestionarea și protejarea resurselor informaționale în cadrul organizațiilor. Acestea includ politici, proceduri și controale pentru gestionarea riscurilor, asigurarea conformității și îmbunătățirea continuă a practicilor de securitate a informațiilor.

F) Gestionarea datelor

Gestionarea datelor se referă la administrarea și supravegherea resurselor informaționale din cadrul unei organizații. Aceasta implică stabilirea de politici, procese și controale pentru calitatea, integritatea și securitatea datelor pentru a se asigura că datele sunt gestionate eficient, responsabil și etic.

G) Răspunsul la incidente și planificarea continuității activității

Răspunsul la incidente și planificarea continuității activității implică pregătirea și răspunsul la incidentele și întreruperile legate de securitatea cibernetică. Startup-urile ar trebui să dezvolte planuri cuprinzătoare de răspuns la incidente și strategii de continuitate a activității pentru a atenua impactul atacurilor cibernetice, al breșelor de date sau al altor perturbări asupra operațiunilor și reputației lor.

Deci, Igiena Digitală cuprinde setul de practici și protocoale care vizează menținerea securității, eficienței și integrității resurselor și operațiunilor digitale. Acest cadru conceptual delimitează componentele cheie ale Igienei Digitale adaptate nevoilor și constrângerilor unice ale startup-urilor.

Schema cadrului conceptual al Igienei Digitale pentru startup-uri este prezentată în figura 1.

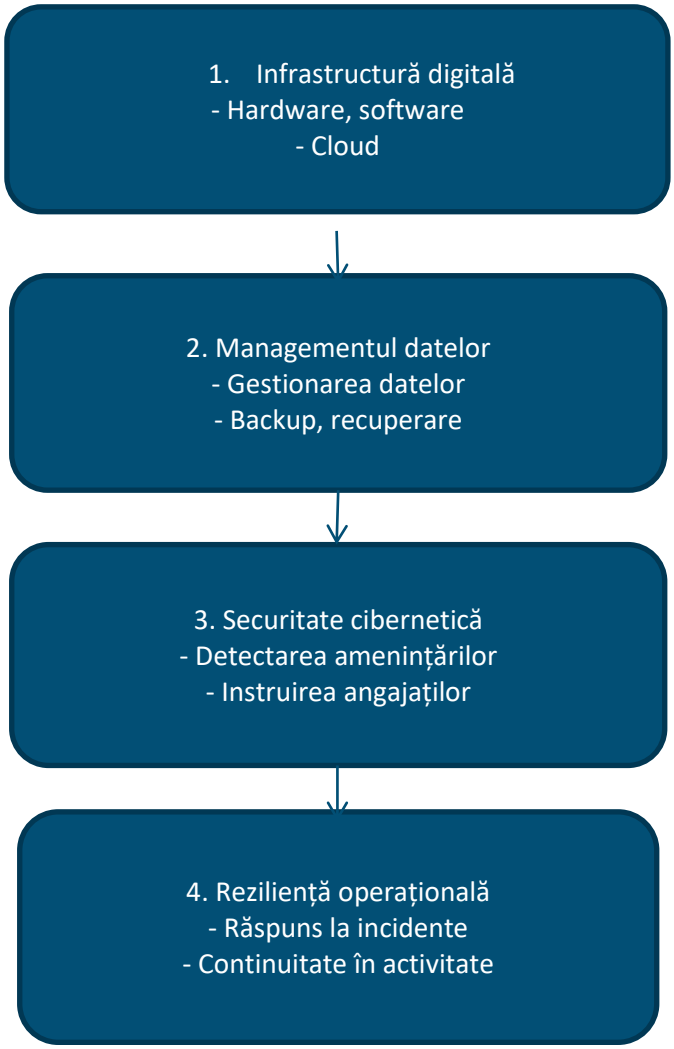


Figura 1. Schema cadrului conceptual al Igienei Digitale pentru startup-uri

Această schemă prezintă cele patru componente principale ale Igienei Digitale pentru startup-uri: infrastructura digitală, gestionarea datelor, securitatea cibernetică și reziliența operațională. Fiecare componentă cuprinde practici și protocoale specifice menite să asigure securitatea, eficiența și integritatea resurselor și operațiunilor digitale într-o organizație de tip startup.

Infrastructura digitală cuprinde hardware-ul, software-ul și serviciile cloud utilizate de startup-uri pentru a-și susține operațiunile și pentru a livra produse sau servicii. Aceasta include dispozitive precum computere, servere și echipamente de rețea, precum și aplicații și platforme software.

Gestionarea datelor implică administrarea, stocarea și protecția resurselor informaționale în cadrul unui startup. Aceasta cuprinde colectarea, stocarea, utilizarea și partajarea datelor, precum și respectarea cerințelor de conformitate și protecția împotriva încălcării datelor.

Securitatea cibernetică se concentrează pe protejarea resurselor și operațiunilor digitale împotriva amenințărilor cibernetice, cum ar fi malware-ul, atacurile de phishing și încercările de acces neautorizat. Aceasta implică implementarea unor măsuri proactive pentru a detecta, preveni și răspunde eficient la incidentele de securitate.

Reziliența operațională implică asigurarea continuității și rezilienței operațiunilor de afaceri în fața unor evenimente perturbatoare, cum ar fi dezastrele naturale, atacurile cibernetice sau defecțiunile sistemului. Aceasta cuprinde măsuri de planificare, pregătire și răspuns pentru a minimiza timpul de nefuncționare și pentru a menține funcțiile critice ale activității.

Figura 2 prezintă procesul de Igienă Digitală și factorii incluși în activitatea startup-urilor.

Această schemă detaliată ilustrează procesul cuprinzător de Igienă Digitală într-un startup, evidențiind factorii și componentele cheie în fiecare etapă, de la evaluare și analiză până la monitorizare și îmbunătățire continuă.

Startup-ul efectuează o evaluare aprofundată a practicilor și vulnerabilităților sale digitale actuale, analizând potențialele riscuri și amenințări la adresa infrastructurii și datelor sale digitale. Pe baza rezultatelor evaluării, startup-ul dezvoltă o strategie cuprinzătoare de Igienă Digitală, adaptată nevoilor și obiectivelor sale, prioritizând domeniile de îmbunătățire.

Startup-ul definește obiective și termene clare pentru implementarea măsurilor de igienă digitală și alocarea eficientă a resurselor, inclusiv bugetul, personalul și tehnologia. Startup-ul oferă sesiuni de instruire și materiale educaționale pentru angajați cu privire la cele mai bune practici de securitate digitală, promovând o cultură a conștientizării și responsabilității securității cibernetice în cadrul organizației.

Startup-ul monitorizează și evaluează continuu eforturile sale de igienă digitală, efectuând audituri și evaluări periodice pentru a identifica zonele de îmbunătățire și adaptare la amenințările și provocările în evoluție.

În concluzie, practicile eficiente de Igienă Digitală sunt indispensabile pentru startup-urile care doresc să navigheze în peisajul complex și dinamic al antreprenoriatului digital. Prin implementarea cadrului conceptual prezentat aici, startup-urile își pot consolida infrastructura digitală, își pot proteja resursele informaționale și își pot îmbunătăți nivelul de securitate cibernetică.

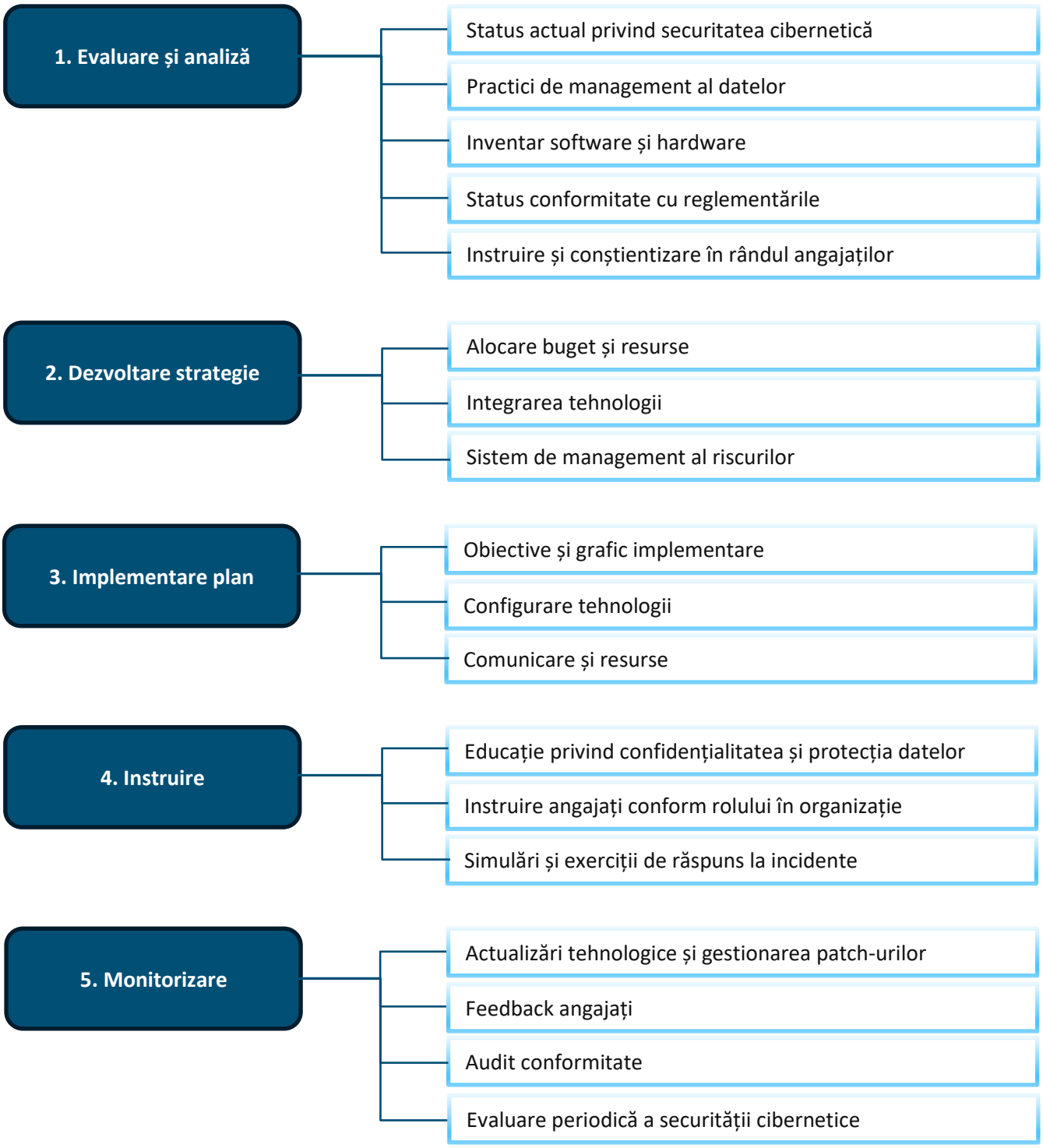


Figura 2. Procesul de Igienă Digitală și factorii incluși în activitatea startup-urilor

Unitatea 2 – Necesitățile/ elementele esențiale ale unei bune Igiene Digitale în startup-uri

În contextul digital actual, startup-urile se bazează foarte mult pe tehnologie pentru a stimula inovația, pentru a eficientiza operațiunile și pentru a ajunge la clienți. Cu toate acestea, odată cu beneficiile tehnologiei vin și riscurile, inclusiv amenințările cibernetice, încălcările datelor și întreruperile operaționale. Pentru a naviga printre aceste provocări și pentru a asigura succesul pe termen lung, startup-urile trebuie să acorde prioritate bunelor practici de Igienă Digitală.

Bunele practici de Igienă Digitală cuprind o serie de măsuri și protocoale proactive menite să protejeze resursele digitale, infrastructura și datele unui startup de potențialele amenințări, vulnerabilități și riscuri.

Necesitățile unei bune igiene digitale pentru startup:

1. Protecția împotriva amenințărilor și atacurilor cibernetice

Unul dintre principalele motive pentru menținerea bunelor practici de Igienă Digitală este protejarea startup-urilor împotriva amenințărilor și atacurilor cibernetice. Într-o eră în care criminalitatea cibernetică este în creștere, startup-urile sunt ținte principale pentru indivizi rău intenționați care încearcă să exploateze vulnerabilitățile din infrastructura și sistemele lor digitale. Atacurile cibernetice, cum ar fi infecțiile malware, escrocheriile de phishing, atacurile ransomware și încălcările datelor, pot avea consecințe devastatoare pentru startup-uri, inclusiv pierderi financiare, daune reputaționale, răspunderi legale și întreruperi operaționale. Prin implementarea unor măsuri consistente de securitate cibernetică, startup-urile își pot consolida apărarea și pot atenua riscurile prezentate de amenințările cibernetice, protejându-și resursele critice și asigurând continuitatea activității.

2. Protejarea datelor sensibile și a proprietății intelectuale

Startup-urile operează frecvent cu date sensibile, inclusiv informații despre clienți, tehnologii brevetate, secrete comerciale și proprietate intelectuală. Menținerea bunelor practici de Igienă Digitală este esențială pentru protejarea acestor informații sensibile împotriva accesului neautorizat, furtului sau compromiterii. Breșele de date și dezvăluirile neautorizate nu numai că pot duce la pierderi financiare și răspunderi legale, ci și la subminarea încrederii clienților, afectând reputația și imaginea brand-ului startup-ului. Prin implementarea criptării datelor, a controalelor de acces și a măsurilor de prevenire a pierderii datelor, startup-urile își pot proteja resursele informaționale sensibile și pot păstra confidențialitatea, integritatea și disponibilitatea acestora, menținând astfel încrederea clienților, partenerilor și stakeholderilor.

3. Creșterea eficienței operaționale și a productivității

Bunele practici de Igienă Digitală contribuie, de asemenea, la creșterea eficienței operaționale și a productivității în cadrul startup-urilor. Software-ul învechit, sistemele fără patch-uri și fluxurile de lucru digitale ineficiente pot îngreuna productivitatea, împiedica colaborarea și încetini creșterea afacerii. Prin menținerea și actualizarea periodică a infrastructurii digitale, startup-urile pot optimiza performanța, eficientiza procesele și elimina blocajele, permițând angajaților să lucreze mai eficient și mai eficace. Mai mult, prin utilizarea automatizării, a tehnologiilor cloud și a instrumentelor digitale, startup-urile pot eficientiza fluxurile de lucru, pot automatiza sarcinile de rutină și pot îmbunătăți procesul decizional, stimulând inovația și competitivitatea pe piață.

4. Asigurarea conformității cu reglementările și obligațiile legale

Respectarea cerințelor de reglementare și a obligațiilor legale este un alt aspect critic al menținerii bunelor practici de igienă digitală. Startup-urile care operează în diverse industrii sunt supuse unei multitudini de legi, reglementări și standarde de conformitate care reglementează confidențialitatea, securitatea și protecția datelor. Nerespectarea acestor reglementări poate duce la sancțiuni severe, amenzi și consecințe juridice, punând în pericol viabilitatea și reputația startup-ului. Prin aderarea la cerințele de reglementare, cum ar fi GDPR, HIPAA, PCI DSS sau SOX, startup-urile își pot demonstra angajamentul față de practicile etice de afaceri, pot câștiga încrederea clienților și a părților interesate, și totodată pot atenua riscurile juridice și financiare.

5. Stimularea inovării

În cele din urmă, menținerea bunelor practici de igienă digitală este esențială pentru stimularea inovării și adaptabilității în cadrul startup-urilor. În contextul economiei digitale actuale, în care progresele tehnologice și perturbările pieței sunt uzuale, startup-urile trebuie să rămână agile, rezistente și adaptabile pentru a prospera într-un peisaj competitiv. Prin adoptarea tehnologiilor emergente, adoptarea transformării digitale și cultivarea unei culturi de îmbunătățire și învățare continuă, startup-urile își pot asigura succesul și sustenabilitatea pe termen lung, stimulând inovarea și creând valoare pentru clienți și stakeholderi.

Pentru a rezuma, menținerea bunelor practici de Igienă Digitală este indispensabilă pentru startup-urile care țintesc spre succes, dezvoltare și sustenabilitate.

.

Unitatea 3 – Importanța Igienei Digitale

Importanța menținerii unei bune Igiene Digitale nu poate fi supraestimată. De la protejarea datelor sensibile la atenuarea amenințărilor cibernetice, practicile de Igienă Digitală sunt esențiale atât pentru indivizi, cât și pentru organizații. În acest studiu de caz, explorăm semnificația Igienei Digitale prin prisma unui exemplu din viața reală, subliniind impactul acesteia asupra securității, productivității și bunăstării generale.

Pentru a înțelege importanța igienei digitale, să trecem în revistă câteva practici de Igienă Digitală.

1. Faceți cunoștință cu TechGenius, un startup dinamic cu sediul în Silicon Valley, specializat în dezvoltarea de soluții software de ultimă generație pentru companii. Fondată în 2015, TechGenius a devenit rapid remarcată în industria tehnologică, atrăgând talente de top și asigurând clienți de profil înalt. Cu toate acestea, pe măsură ce compania și-a extins operațiunile și forța de muncă, s-a confruntat cu noi provocări în gestionarea infrastructurii sale digitale și protejarea resurselor sale digitale.

TechGenius, la fel ca multe startup-uri, a funcționat într-un mediu rapid, în care inovarea și eficiența au fost primordiale. Cu toate acestea, în mijlocul agitației operațiunilor zilnice, compania a neglijat să acorde prioritate practicilor de Igienă Digitală. Angajații au folosit adesea parole slabe, nu au reușit să actualizeze software-ul în mod regulat și au ignorat protocoalele de securitate de bază, lăsând compania vulnerabilă la amenințările cibernetice, cum ar fi atacurile de phishing și încălcări ale datelor.

Realizând importanța critică a Igienei Digitale, TechGenius s-a angajat într-un demers susținut pentru a-și reînnoi abordarea în ceea ce privește securitatea cibernetică și gestionarea datelor. Compania a lansat o amplă inițiativă de Igienă Digitală menită să educe angajații, să implementeze cele mai bune practici și să-și consolideze poziția de securitate.

Inițiativa de igienă digitală a TechGenius a cuprins mai multe componente cheie:

1. Instruirea și conștientizarea angajaților. Compania a desfășurat sesiuni de instruire ample pentru a educa angajații cu privire la importanța Igienei Digitale. Subiectele abordate au inclus gestionarea parolelor, securitatea e-mailurilor, practicile de navigare sigură și reglementările privind protecția datelor. Prin ateliere interactive și module online, angajații au dobândit o înțelegere mai profundă a riscurilor de securitate cibernetică și a rolului lor în atenuarea acestora.

2. Elaborarea și punerea în aplicare a politicilor. TechGenius a dezvoltat politici și proceduri puternice de Igienă Digitală pentru a gestiona comportamentul angajaților și pentru a asigura conformitatea cu standardele industriei. Aceste politici au abordat domenii precum complexitatea parolelor, actualizările software, controalele de acces și protocoalele de răspuns la incidente. Pentru a consolida responsabilitatea,

compania a implementat audituri periodice și mecanisme de aplicare pentru a monitoriza respectarea acestor politici.

3. Soluții tehnologice. Pe lângă măsurile educaționale și politice, TechGenius a investit în soluții tehnologice pentru a-și îmbunătăți practicile de Igienă Digitală. Aceasta a inclus implementarea autentificării multi-factor, a tehnologiilor de criptare, a software-ului de securitate a punctelor finale și a instrumentelor de monitorizare a rețelei. Prin utilizarea acestor tehnologii, compania și-a consolidat apărarea împotriva amenințărilor cibernetice și și-a protejat infrastructura digitală.

Implementarea inițiativei de igienă digitală TechGenius a dat rezultate semnificative:

A. Politică de Securitate îmbunătățită. Prin prioritizarea Igienei Digitale, TechGenius și-a consolidat abordarea privind securitatea și a redus riscul amenințărilor cibernetice. Incidente precum atacurile de phishing și breșele de date au devenit mai puțin frecvente, minimizând impactul potențial asupra operațiunilor și reputației companiei.

B. Productivitate sporită. Cu mai puține incidente de securitate cu care să se confrunte, angajații au putut să se concentreze mai mult asupra responsabilităților lor de bază, ceea ce a dus la creșterea productivității și eficienței în întreaga organizație. Prin eficientizarea fluxurilor de lucru digitale și minimizarea timpilor morți, TechGenius a obținut rezultate mai bune și a oferit rezultate superioare clienților săi.

C. Reputație protejată. În calitate de furnizor de încredere de soluții software, reputația TechGenius depinde de capacitatea sa de a proteja datele clienților și de a menține standarde înalte de securitate. Prin demonstrarea unui angajament față de Igiena Digitală, compania a câștigat încrederea clienților săi, poziționându-se ca un partener de încredere pe o piață din ce în ce mai competitivă.

D. Economii de costuri. În timp ce investiția în Igiena Digitală poate implica costuri inițiale, beneficiile pe termen lung depășesc cu mult cheltuielile. TechGenius a înregistrat economii de costuri în ceea ce privește reducerea incidentelor de securitate cibernetică, reducerea penalităților de conformitate și creșterea eficienței operaționale. Prin abordarea proactivă a vulnerabilităților de securitate, compania a evitat repercusiunile potențial costisitoare asociate cu încălcarea datelor și nerespectarea reglementărilor.

Cazul TechGenius subliniază importanța critică a igienei digitale în contextual digital actual. Prin prioritizarea educației în domeniul securității cibernetice, a dezvoltării politicilor și a soluțiilor tehnologice, TechGenius a reușit să atenueze amenințările cibernetice, să sporească productivitatea și să-și protejeze reputația. Acest exemplu din viața reală servește drept dovadă a puterii transformatoare a Igienei Digitale în protejarea organizațiilor împotriva riscurilor cibernetice în evoluție și în stimularea creșterii durabile și a succesului.

2. Un alt exemplu al importanței practicilor de igienă digitală este cazul SecureHealth.

SecureHealth este un startup de tehnologie medicală care revoluționează modul în care sunt gestionate și accesate dosarele medicale. Cu o platformă bazată pe cloud, concepută pentru a eficientiza îngrijirea pacienților și pentru a îmbunătăți rezultatele asistenței medicale, SecureHealth a câștigat rapid teren în industria asistenței medicale. Cu toate acestea, în mijlocul creșterii rapide și adoptării platformei sale, compania se confruntă cu provocări semnificative în asigurarea securității și confidențialității datelor pacienților.

Organizațiile din domeniul sănătății sunt ținte principale pentru atacurile cibernetice datorită naturii sensibile a datelor pe care le gestionează. SecureHealth recunoaște importanța critică a Igienei Digitale în protejarea confidențialității pacienților și menținerea conformității cu reglementările. Cu toate acestea, având în vedere complexitatea sistemelor IT din domeniul sănătății și tipurilor de amenințări în continuă evoluție, compania trebuie să rămână vigilentă și proactivă în abordarea riscurilor de securitate cibernetică.

SecureHealth adoptă o abordare proactivă a Igienei Digitale, implementând un program cuprinzător de securitate cibernetică adaptat nevoilor unice ale industriei medicale. Compania prioritizează următoarele componente cheie:

1. Criptarea datelor și controlul accesului. SecureHealth criptează datele pacienților, asigurându-se că informațiile sensibile rămân protejate împotriva accesului neautorizat. Controalele de acces sunt implementate pentru a restricționa accesul la înregistrările pacienților numai profesioniștilor autorizați din domeniul sănătății, minimizând riscul de încălcare a datelor.

2. Audituri periodice de securitate și teste de penetrare. SecureHealth efectuează audituri regulate de securitate și teste de penetrare pentru a identifica vulnerabilitățile din sistemele și infrastructura sa. Prin identificarea proactivă și remedierea punctelor slabe de securitate, compania își consolidează apărarea împotriva amenințărilor cibernetice și asigură conformitatea cu reglementările din domeniul sănătății, cum ar fi HIPAA.

3. Instruirea și conștientizarea angajaților. SecureHealth oferă instruire amplă în domeniul securității cibernetice tuturor angajaților, subliniind importanța Igienei Digitale în protejarea datelor pacienților. Angajații învață cum să recunoască și să răspundă amenințărilor de securitate, să implementeze practici sigure în fluxurile lor zilnice de lucru și să adere la politicile și procedurile companiei.

Implementarea inițiativelor de Igienă Digitală ale SecureHealth a dat rezultate tangibile:

A. Datele pacienților sunt protejate. Prin prioritizarea Igienei Digitale, SecureHealth asigură confidențialitatea, integritatea și disponibilitatea datelor pacienților, promovând încrederea în rândul furnizorilor de servicii medicale și al pacienților deopotrivă.

B. Respectarea reglementărilor. SecureHealth menține conformitatea cu reglementările din domeniul sănătății, cum ar fi HIPAA, demonstrând angajamentul său de a proteja confidențialitatea pacienților și de a îndeplini standardele industriei privind securitatea și confidențialitatea datelor.

C. Risc redus de încălcare a securității datelor. Cu măsuri consistente de securitate cibernetică, SecureHealth minimizează riscul de încălcare a datelor și alte incidente de securitate, protejându-și reputația și minimizând potențialele consecințe financiare și juridice.

Experiența SecureHealth evidențiază importanța critică a Igienei Digitale în industria medicală, unde mizele sunt mari, iar consecințele breșelor de securitate pot fi grave. Prin prioritizarea măsurilor de securitate cibernetică, cum ar fi criptarea datelor, controlul accesului, auditurile periodice și instruirea angajaților, SecureHealth asigură securitatea și integritatea datelor pacienților, contribuind în cele din urmă la îmbunătățirea îngrijirii pacienților și a rezultatelor.

Pentru a înțelege semnificația igienei digitale, luați în considerare examinarea practicilor suplimentare de igienă digitală.

3. FinTech Innovations este un startup care revoluționează industria serviciilor financiare cu soluții bancare digitale inovatoare. Folosind tehnologii de ultimă oră, cum ar fi blockchain și inteligența artificială, FinTech Innovations oferă servicii bancare sigure și ușor de utilizat atât consumatorilor, cât și companiilor. Cu toate acestea, pe măsură ce organizația crește și își extinde baza de clienți, se confruntă cu riscuri tot mai mari de securitate cibernetică care amenință securitatea și stabilitatea platformei sale.

Instituțiile financiare sunt ținte principale pentru atacurile cibernetice datorită datelor financiare valoroase pe care le dețin. FinTech Innovations recunoaște importanța Igienei Digitale în menținerea încrederii clienților și partenerilor săi. Cu toate acestea, având în vedere complexitatea tranzacțiilor financiare și natura evolutivă a amenințărilor cibernetice, compania trebuie să rămână vigilentă și proactivă în protejarea activelor și infrastructurii sale digitale.

FinTech Innovations implementează un program robust de Igienă Digitală pentru a aborda riscurile de securitate cibernetică și pentru a-și proteja platforma. Compania se concentrează pe următoarele inițiative cheie:

1. Autentificare și autorizare securizate. FinTech Innovations implementează mecanisme puternice de autentificare, cum ar fi autentificarea biometrică și autentificarea multi-factor, pentru a verifica identitatea utilizatorilor și pentru a preveni accesul neautorizat la conturi și tranzacții.

2. Detectarea fraudei în timp real. FinTech Innovations utilizează algoritmi avansați de analiză și învățare automată pentru a detecta și preveni activitățile frauduloase în timp real. Prin analizarea modelelor de

tranzacții și a comportamentului utilizatorilor, compania poate identifica activitățile suspecte și poate lua măsuri proactive pentru a atenua riscurile de fraudă.

3. Monitorizare continuă. FinTech Innovations menține monitorizarea continuă a sistemelor și rețelelor sale pentru a detecta și a răspunde prompt la incidentele de securitate. Compania are o echipă dedicată de profesioniști în domeniul securității cibernetice care monitorizează activitățile suspecte, investighează alertele de securitate și implementează acțiuni de remediere în timp util pentru a aborda potențialele amenințări.

Implementarea inițiativelor de Igienă Digitală ale FinTech Innovations a condus la rezultate semnificative:

A. Creșterea încrederii clienților. Prin prioritizarea Igienei Digitale, FinTech Innovations își demonstrează angajamentul de a proteja datele clienților și activele financiare, construind încredere în rândul utilizatorilor și stakeholderilor.

B. Reducerea fraudei și a incidentelor de securitate. Cu mecanisme avansate de detectare a fraudelor și monitorizare continuă, FinTech Innovations minimizează riscul de fraudă și incidente de securitate, asigurând securitatea și integritatea platformei și tranzacțiilor sale.

C. Continuitatea și reziliența activității. Prin abordarea proactivă a riscurilor de securitate cibernetică, FinTech Innovations își îmbunătățește reziliența la amenințările și perturbările cibernetice, asigurând furnizarea neîntreruptă de servicii financiare clienților și partenerilor săi.

Experiența FinTech Innovations subliniază importanța critică a Igienei Digitale în industria serviciilor financiare, unde securitatea și încrederea sunt primordiale. Prin implementarea unor măsuri complexe de securitate cibernetică, cum ar fi autentificarea securizată, detectarea fraudelor și monitorizarea continuă, FinTech Innovations asigură securitatea și stabilitatea platformei sale, contribuind în cele din urmă la o experiență bancară digitală mai sigură pentru clienții săi

Aceste exemple ilustrează rolul vital al Igienei Digitale în protejarea datelor sensibile, menținerea conformității cu reglementările și protejarea împotriva amenințărilor cibernetice în diverse industrii, cum ar fi asistența medicală și finanțele. Prioritizarea igienei digitale este esențială pentru organizațiile care doresc să atenueze riscurile, să construiască încredere și să stimuleze creșterea durabilă și succesul în contextul digital actual.

Unitatea 4 – Un exemplu de bune practici din startup-uri

Pentru a ilustra identificarea eficientă a amenințărilor și măsurile preventive, vom aprofunda un exemplu care pune accentul pe instruirea în domeniul securității cibernetice pentru angajați. Acest exemplu servește pentru a sublinia rolul critic al educației angajaților în susținerea măsurilor de securitate digitală.

CyberSec Europe

Context

CyberSec Europe este un startup de securitate cibernetică cu sediul în Berlin, Germania, specializat în furnizarea de soluții de securitate pentru întreprinderile mici și mijlocii (IMM-uri). Fondată în 2017, CyberSec Europe s-a impus rapid ca un furnizor de încredere de servicii de securitate cibernetică pe piața europeană. Pe măsură ce compania a crescut și și-a extins baza de clienți, a recunoscut importanța critică a educației în domeniul securității cibernetice pentru angajații săi.

În ciuda faptului că are o echipă de profesioniști calificați în domeniul securității cibernetice, CyberSec Europe a identificat necesitatea de a spori gradul de conștientizare al angajaților săi cu privire la cele mai bune practici de securitate cibernetică. Odată cu creșterea gradului de sofisticare a amenințărilor cibernetice și adoptarea programului de lucru la distanță, riscul de incidente de securitate, cum ar fi atacurile de phishing și breșele de date, a crescut. CyberSec Europe a înțeles că educarea angajaților săi cu privire la riscurile și protocoalele de securitate cibernetică este esențială pentru menținerea reputației sale de furnizor de încredere în domeniul securității cibernetice.

Soluția

CyberSec Europe a implementat un program cuprinzător de instruire în domeniul securității pentru toți angajații, concentrându-se pe domenii cheie, cum ar fi detectarea amenințărilor, răspunsul la incidente și respectarea reglementărilor privind protecția datelor (de exemplu Regulamentul general privind protecția datelor - GDPR). Programul de instruire a fost conceput pentru a fi interactiv, antrenant și adaptat nevoilor specifice ale forței de muncă a CyberSec Europe.

Programul de instruire în domeniul securității a fost desfășurat la nivelul întregii companii pe parcursul a trei luni. Acesta a constat într-o serie de ateliere, webinare și exerciții practice conduse de experți interni în domeniul securității cibernetice și consultanți externi. Subiectele abordate în programul de formare au inclus:

- ✓ Identificarea și răspunsul la e-mailurile de tip phishing
- ✓ Crearea și gestionarea parolelor puternice
- ✓ Recunoașterea semnelor comune ale atacurilor cibernetice

- ✓ Protejarea datelor sensibile și asigurarea conformității cu GDPR
- ✓ Raportarea incidentelor de securitate și respectarea procedurilor de răspuns la incidente

Pentru a încuraja participarea și implicarea, CyberSec Europe a stimulat angajații să finalizeze modulele de instruire și a oferit recompense pentru performanța exemplară în exercițiile de conștientizare a importanței securității. Compania a oferit, de asemenea, sprijin continuu și resurse angajaților, cum ar fi accesul la instrumente de securitate cibernetică și resurse online.

Implementarea instruirii periodice în domeniul securității a dat rezultate pozitive pentru CyberSec Europe:

1. Creșterea gradului de conștientizare a securității. Angajații au devenit mai vigilenți și mai informați cu privire la riscurile de securitate cibernetică, ceea ce a dus la o reducere a incidentelor de securitate și a încălcărilor de date.

2. Practici de securitate îmbunătățite. Angajații au adoptat cele mai bune practici în domeniul securității cibernetice, cum ar fi utilizarea parolelor puternice, criptarea datelor sensibile și raportarea promptă a activităților suspecte.

3. Creșterea încrederii clienților. Angajamentul CyberSec Europe față de educația în domeniul securității cibernetice a demonstrat dedicarea sa pentru protejarea datelor și confidențialității clienților, sporind încrederea și credibilitatea în rândul clienților săi.

4. Gradul de pregătire pentru conformitate. Prin educarea angajaților cu privire la cerințele GDPR și alte standarde de reglementare, CyberSec Europe și-a îmbunătățit poziția de conformitate și a minimizat riscul sancțiunilor de reglementare.

Abordarea proactivă a CyberSec Europe în ceea ce privește educația în domeniul securității cibernetice subliniază importanța instruirii regulate în domeniul securității pentru startup-urile din Europa. Investind în conștientizarea și responsabilizarea angajaților, CyberSec Europe a reușit să-și consolideze apărarea cibernetică, să atenueze riscurile și să câștige încrederea clienților. Acest exemplu din viața reală evidențiază eficacitatea formării în domeniul securității cibernetice pentru îmbunătățirea Igienei Digitale și protejarea startup-urilor împotriva amenințărilor cibernetice.

Asigurarea bunelor practici de Igienă Digitală este esențială pentru ca startup-urile din Europa să prospere în contextul digital actual. Prevalența crescândă a amenințărilor cibernetice, a încălcării datelor și a cerințelor de reglementare subliniază importanța prioritizării securității cibernetice, a protecției datelor și a eforturilor de conformitate. Prin implementarea unor măsuri complexe de Igienă Digitală, startup-urile își pot proteja resursele digitale, pot proteja datele sensibile și pot obține încrederea clienților, partenerilor și stakeholderilor. Cu toate acestea, implementarea și menținerea unei bune Igiene Digitale necesită un efort concertat, vigilență permanentă și un angajament pentru îmbunătățirea continuă.

Recomandări pentru îmbunătățirea igienei digitale a startup-urilor din Europa

✓ Se recomandă ca startup-urile să efectueze evaluări periodice ale practicilor proprii de Igienă Digitală, inclusiv politica de securitate cibernetică, protocoalele de gestionare a datelor și nivelul de conformitate cu reglementările. Acest lucru va ajuta la identificarea vulnerabilităților, a lacunelor și a domeniilor care necesită îmbunătățiri.

✓ Pe baza rezultatelor evaluării, este recomandabil ca startup-urile să dezvolte strategii cuprinzătoare de Igienă Digitală, adaptate nevoilor, obiectivelor și profilurilor lor specifice de risc. Strategiile ar trebui să abordeze domenii-cheie, cum ar fi securitatea cibernetică, protecția datelor, conformitatea și răspunsul la incidente.

✓ Se recomandă ca startup-urile să investească în tehnologii și soluții de securitate cibernetică pentru a-și proteja infrastructura digitală de amenințările cibernetice, malware și breșele de date. Acestea pot include firewall-uri, software antivirus, tehnologii de criptare și sisteme de detectare a intruziunilor.

✓ Startup-urile ar trebui să acorde prioritate protecției datelor și confidențialității prin implementarea unor protocoale complexe de gestionare a datelor, inclusiv criptarea, controlul accesului și mecanismele de backup și recuperare a datelor. Respectarea reglementărilor precum GDPR este esențială pentru startup-urile care gestionează date cu caracter personal.

✓ Este recomandabil ca startup-urile să promoveze conștientizarea și educarea securității cibernetice în rândul angajaților pentru a se asigura că înțeleg riscurile potențiale, cele mai bune practici și procedurile pentru menținerea unei bune Igiene Digitale. Sesiunile regulate de instruire, campaniile de sensibilizare și simulările de phishing pot contribui la consolidarea gradului de conștientizare a securității cibernetice.

✓ Startup-urile ar trebui să dezvolte și să implementeze planuri de răspuns la incidente pentru a răspunde eficient la incidente de securitate cibernetică, încălcări ale datelor sau alte situații de urgență. Planurile ar trebui să sublinieze rolurile, responsabilitățile și procedurile pentru detectarea, limitarea și atenuarea incidentelor.

✓ Monitorizarea și evaluarea continuă sunt esențiale pentru menținerea unei bune Igiene Digitale. Se recomandă ca startup-urile să evalueze în mod regulat eficacitatea măsurilor lor de Igienă Digitală, să efectueze audituri și revizuiri și să facă ajustările necesare pentru a aborda amenințările și provocările emergente.

✓ Startup-urile ar trebui să rămână informate cu privire la cele mai recente amenințări la adresa securității cibernetice, tendințele și reglementările care afectează industria lor. Monitorizarea regulată a știrilor despre securitatea cibernetică, participarea la forumuri din industrie și colaborarea cu profesioniștii din domeniul securității cibernetice pot ajuta startup-urile să fie cu un pas înaintea amenințărilor și riscurilor în evoluție.

Pentru a rezuma, îmbunătățirea practicilor de Igienă Digitală este esențială pentru startup-urile din Europa pentru a-și proteja resursele digitale, pentru a atenua riscurile și pentru a păstra încrederea stakeholderilor. Prin implementarea unor strategii ample, investiții în tehnologii de securitate cibernetică, promovarea conștientizării și monitorizarea, respectiv adaptarea continuă la amenințările în schimbare, startup-urile își pot consolida reziliența digitală și pot prospera într-un peisaj competitiv.

De reținut

- Se recomandă ca startup-urile să acorde prioritate educației în domeniul securității cibernetice pentru angajații lor, pentru a crește gradul de conștientizare și pentru a-i împuternici să recunoască și să răspundă eficient la amenințările cibernetice. Programele de instruire ar trebui să acopere subiecte precum conștientizarea phishingului, gestionarea parolelor și protocoalele de răspuns la incidente.
- Stabilirea unor politici și proceduri solide de Igienă Digitală este esențială pentru promovarea unei culturi a securității cibernetice în cadrul companiilor nou-înființate. Este recomandabil să se dezvolte politici care să abordeze domenii precum complexitatea parolelor, actualizările software, controalele de acces și reglementările privind protecția datelor.
- Auditurile regulate și mecanismele de aplicare ajută la asigurarea conformității și responsabilității în cadrul startup-urilor. Se recomandă efectuarea de audituri periodice și implementarea mecanismelor de aplicare pentru a monitoriza respectarea politicilor și procedurilor de Igienă Digitală.
- Startup-urile ar trebui să investească în soluții tehnologice pentru a-și îmbunătăți practicile de Igienă Digitală. Aceasta include implementarea instrumentelor de securitate cibernetică, cum ar fi autentificarea multi-factor, tehnologiile de criptare, software-ul de securitate al dispozitivelor de lucru și instrumentele de monitorizare a rețelei pentru a consolida apărarea împotriva amenințărilor cibernetice.
- Respectarea cerințelor de reglementare și a standardelor din industrie este esențială pentru ca startup-urile să-și demonstreze angajamentul față de practicile etice de afaceri și să se protejeze împotriva repercusiunilor legale și financiare. Startup-urile ar trebui să respecte reglementări precum GDPR, HIPAA, PCI DSS sau SOX pentru a proteja confidențialitatea, securitatea și integritatea datelor.
- Conceptul de igienă digitală integrează perspective din diferite discipline, inclusiv securitatea cibernetică, managementul informațiilor, factorii umani, comportamentul organizațional și teoria conformității. Bazându-se pe aceste perspective, startup-urile pot dezvolta abordări pentru a aborda în mod eficient provocările complexe ale securității cibernetice și ale protecției datelor.

Referințe:

1. CyberSec Europe https://www.cyberseceurope.com/
2. FinTech Innovations https://www.fintechinnovation.no/
3. Ncubukezi T., Mwansa L. Best Practices Used by Businesses to Maintain Good Cyber Hygiene During Covid-19 Pandemic. Journal of Internet Technology and Secured Transactions (JITST), Volume 9, Issue 1, 2021.
4. SecureHealth https://www.shpg.com/
5. TechGenius https://techgenius.co.in/
6. Vishwanath A., Seng Neo L., Goh P., Lee S., Khader M., Ong G., Chin. J. Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, Volume 128, 2020, https://doi.org/10.1016/j.dss.2019.113160.
7. Yegen, C., Kirik, A.M., Çetinkaya, A. (2023). Sustainability, Digital Security, and Cyber Hygiene During the Covid-19 Pandemic. In: Mondal, S.R., Yegen, C., Das, S. (eds) New Normal in Digital Enterprises. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-19-8618-5_5

Modulul 2 – Instrumente de Igienă Digitală & Integrarea în rutina zilnică

Unitatea 1- Instrumente de top de Igienă Digitală pentru Startup-uri

O lume interconectată prezintă riscuri de amenințări digitale mai ample și mai complicate. De aceea, este mai important ca niciodată ca startup-urile să acorde o importanță substanțială securității cibernetice pentru a-și proteja resursele valoroase și informațiile confidențiale. În această Unitate, veți afla despre unele dintre strategiile și practicile cheie pe care startup-urile ar trebui să încerce să le implementeze pentru a-și îmbunătăți securitatea online. Acestea variază de la crearea de parole puternice până la implementarea unor soluții complete de backup de date. Acest ghid vă va oferi cunoștințele și instrumentele pe care startup-urile trebuie să le cunoască pentru a rămâne în siguranță online. Această Unitate vă va ghida prin principiile cheie și vă va oferi o serie de recomandări care vă vor ajuta să construiți o bază solidă pentru strategia dvs. de Igienă Digitală, precum și să vă protejați resursele digitale în mod eficient.

1.1 Menținerea unei igiene bune a parolelor: elementele de bază

Compania Ticketmaster a fost dat în judecată în ianuarie 2021 pentru hacking-ul sistemelor informatice ale unei companii rivale, după ce un fost angajat al companiei rivale și-a folosit acreditările pentru a permite Ticketmaster să aibă acces clandestin la computerele concurentului său. Procurorul american interimar DuCharme a declarat că "angajații Ticketmaster au accesat ilegal computerele unui concurent fără permisiune, în numeroase ocazii, pentru a fura cunoștințe comerciale prin parole obținute ilegal". Acest caz singular a dus la faptul că Ticketmaster a fost supus unei penalități în numerar de 10 milioane de dolari în conformitate cu termenii Legii privind frauda și abuzul informatic. (Jones, 2022) Raportul Google Cloud Threat Horizons 2023 indică faptul că 86% dintre breșele de securitate includ utilizarea acreditărilor furate, iar problemele legate de acreditări sunt responsabile pentru mai mult de 60% din cauzele care stau la baza breșelor – probleme pe care flancurile mai puternice de gestionare a identității organizaționale le-ar putea ajuta să le rezolve. După părerea lui Keszthely (2013), actul de a lua parola altcuiva poate fi completat în patru moduri de bază:

1- Cuvinte implicite: Computerele și aplicațiile au parole implicite încorporate. Parolele pentru computer și cont pot fi nule sau pot face parte dintr-un set separat de cuvinte comune, cum ar fi "123456", "asdfgh" și "parolă".

2- Conexiune între numele de conectare și parole: Ghicirea parolei sau logica este atunci când atacatorii vor aloca timp special pentru a ghici sistematic numele de utilizator și parola. Utilizatorul poate chiar ajuta atacatorul să ghicească numele de utilizator și parola. Câteva exemple sunt "parola", "autentificare-autentificare", "qwerty" și "letmein".

3- Metoda dicționarului: Hackerii vor colecta câteva parole generale și le vor selecta din listă. Le vor descărca pe rând, deoarece instrumentele funcționează offline și au mai multe șanse să reușească dacă funcționează mai lent. În plus, vor avea în continuare posibilitatea de a testa fiecare componentă fără o conexiune la Internet.

Pentru a evita daune cauzate de furtul parolei, este necesar să acordați prioritate selecției parolelor puternice și sigure. Kato și Klyuev (2013) sugerează câteva sfaturi recomandate pentru crearea parolelor puternice:

- **Utilizați majuscule și semne de punctuație**: Utilizați litere mari și semne de punctuație pentru a crea o parolă mai puternică.
- **Amestecați:** Integrați atât litere, cât și numere pentru a genera parole mai sigure.
- **Evitați informațiile frecvente**: Abțineți-vă de la utilizarea cuvintelor ușor de ghicit și a detaliilor informațiilor personale în parole.
- **Luați în considerare parole mai lungi:** Vizați parole mai lungi, ușor de reținut.
- **Utilizați manageri de parole**: Utilizați programe concepute pentru a stoca parolele în siguranță, cum ar fi LastPass.
- **Parole unice**: Formulați parole diferite pentru conturi diferite.

Pe lângă setarea unor parole sigure la nivel de indivizi, companiile trebuie să implementeze politici care să se concentreze pe îmbunătățirea securității parolelor. La nivel organizațional, liniile directoare privind parolele ar trebui să se concentreze în jurul utilizatorului. Regulile de setare ar trebui să reflecte cerințele și competențele unice ale utilizatorilor în activitatea lor de zi cu zi. Organizațiile pot maximiza securitatea, consolidând în același timp eficacitatea și eficiența utilizatorilor în gestionarea parolelor, respectând principiile interacțiunii om-computer și ținând cont de utilizarea specifică. În plus, companiile ar trebui să încerce să analizeze și să aplice standarde stricte de creare a parolelor utilizând noi tehnici și dispozitive de parolă precum Telepathwords. De asemenea, organizațiile ar trebui să se asigure că instruiesc angajații să

nu utilizeze parole slabe sau ușor de intuit. Depășirea schemei prin aceste tehnici va îmbunătăți foarte mult siguranța (Inglesant & Sasse, 2010; Blocki & Liu, 2023).

1.2 Protejarea structurii vitale folosind Autentificarea cu doi factori

Autentificarea cu doi factori (2FA) este o măsură de securitate care impune utilizatorilor să furnizeze o componentă secundară pentru confirmarea utilizatorului. Această metodă adaugă un factor de autentificare la sistemul de autentificare cu parolă. Implementarea 2FA prezintă o serie de avantaje precum (Tellini & Vargas, 2017) :

- **Eliminarea posibilității accesului neautorizat**: 2FA depășește simpla utilizare a unui nume de utilizator și a unei parole. Utilizează un sistem complet separat pentru autentificare.
- **Protecție împotriva furtului de parole:** Numele de utilizator și parolele sunt furate zilnic. Cu 2FA, un atacator ar avea nevoie de mai mult decât doar numele utilizatorului și acreditările parolei pentru a obține acces nelegitim.
- **Risc scăzut de acces neautorizat**: Cu 2FA, accesul neautorizat sau nedovedit este mai puțin probabil din cauza stratului suplimentar de autentificare de care hackerul ar avea nevoie pentru a finaliza accesarea contului și ar avea nevoie de posesia telefonului utilizatorului sau a unui cod generat pe telefonul acestuia.
- **Creșterea încrederii utilizatorilor:** Încrederea în software poate crește atunci când utilizatorii știu că contul lor este protejat de mai mult decât o parolă.
- **Respectarea standardelor de securitate:** Utilizarea 2FA vă poate face conectările conforme cu cele mai bune practici pentru securitatea online și poate fi impusă de reglementări sau standarde specifice din industria dvs.
- **Atenuarea problemelor comune legate de parole:** 2FA ajută la atenuarea problemelor comune legate de parole, cum ar fi alegerile slabe ale parolei și reutilizarea. Prin reducerea dependenței noastre de o singură parolă, 2FA ne poate ajuta să folosim parole mai complexe.

2FA este un proces de verificare în doi pași care solicită utilizatorilor să furnizeze două tipuri diferite de factori de autentificare înainte de a acorda acces utilizatorului final. Factorii pot include: ceva ce utilizatorul știe (factorul de cunoștințe), ceva ce utilizatorul are (factorul de posesie) și ceva ce utilizatorul este (factorul de inerență). Metoda de autentificare cu doi factori face ca tehnicile de autentificare centrate pe parolă să fie mai sigure. Serviciile pot utiliza combinații dinamice de factori pentru a spori considerabil asigurarea acreditării utilizatorilor prin cuantificarea riscurilor și beneficiilor. (De Cristofaro, Du, Freudiger, & Norcie, 2013; Han, Sun, Shen, Chang, & Shen, 2013).

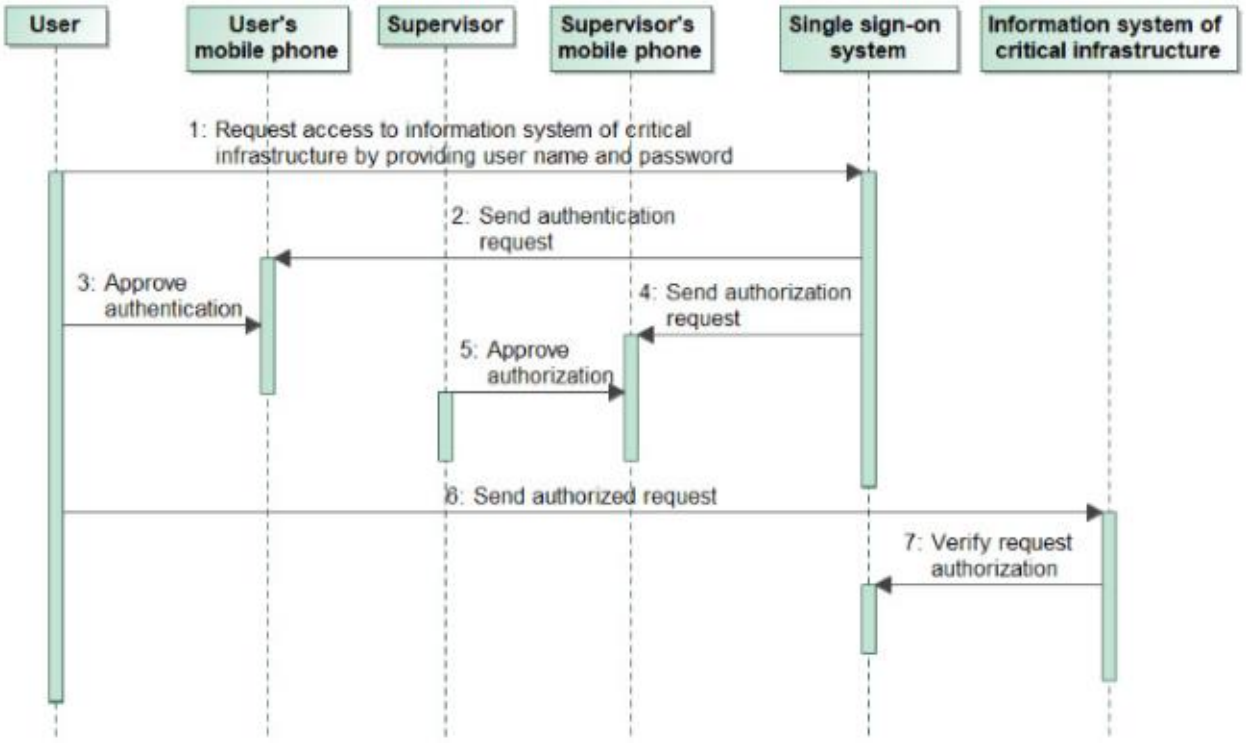
Class type	Class description	Examples
Knowledge	Something known	Password Key phrase Secret question Personal question
Possession	Something held	One time password generator Grid token Smart card
Inherence (biometrics)	Something about the person	Fingerprint scan Iris scan Voice recognition

Tabelul 1: Câteva exemple de categorii de factori care pot fi utilizați pentru autentificarea multifactor

Sursa : (Pearce, Zeadally, & Hunt, 2010).

Bruzgiene & Jurgilas (2019) oferă o metodă de autentificare care funcționează într-un proces în trei pași pentru securizarea accesului de la distanță la sistemele informatice ale infrastructurii critice. În primul rând, utilizatorul introduce ID-ul contului și parola. Odată ce informațiile corecte sunt introduse, o solicitare de autentificare de la autoritatea locală de securitate (LSA) va fi trimisă pe dispozitivul mobil al utilizatorului. Apoi, utilizatorul trebuie să aprobe cererea printr-o singură atingere a ecranului telefonului. Acest lucru va permite dispozitivului mobil să trimită o cerere de autorizare supraveghetorului (supraveghetorilor) utilizatorului pentru a determina nivelul drepturilor de acces pentru sistemul la distanță. Odată ce cererea utilizatorului este aprobată cu succes de către supraveghetor (supraveghetori), utilizatorului solicitant i se acordă drepturi de acces la sistemul la distanță.

Figura 1: Metoda de autentificare propusă de (Bruzgiene & Jurgilas, 2019)



Sursa: (Bruzgiene & Jurgilas, 2019)

1.3 Actualizări software în timp util: consolidarea securității sistemului

Actualizările software sunt foarte importante, deoarece remediază erorile sau îmbunătățesc performanța software-ului, cum ar fi driverele și sistemele de operare. Prin actualizarea software-ului, vă asigurați că este compatibil cu alte sisteme software și hardware și vă păstrați sistemele în siguranță rulând cea mai recentă versiune a software-ului. Actualizările cuprind actualizări de securitate care sunt necesare pentru a proteja un computer de software rău intenționat și vulnerabilități, actualizări de caracteristici care variază în ceea ce privește severitatea, deoarece pot include orice, de la remedieri minore de erori la modificări semnificative ale fluxului de lucru și actualizarea cumulativă care necesită instalarea tuturor actualizărilor anterioare înainte de a ajunge la cea mai recentă actualizare (Mathur, Malkin, Harbach, Péer, & Egelman, 2018; Vaniea, Rader, & Wash, 2014). Aceste îmbunătățiri ajută la menținerea securității și funcționalității sistemelor software. Din acest motiv, este important să vă asigurați că sunteți la curent cu toate actualizările necesare.

Cu toate acestea, mulți utilizatori tind să evite actualizarea software-ului din cauza factorilor percepuți. Acești factori includ: *Costuri de actualizare*, cum ar fi timpul de instalare, care necesită repornire și spațiul pe disc utilizat; *Necesitatea actualizării*, inclusiv satisfacția utilizatorului față de sistemul actual, claritatea motivelor actualizării și importanța actualizării percepute ca fiind percepută de utilizator și *Riscul de actualizare* care implică îngrijorări cu privire la pierderea datelor în timpul actualizărilor și că orice actualizare ar putea purta un virus sau malware care ar putea face un sistem vulnerabil (Mathur, Malkin, Harbach, Péer, & Egelman, 2018). Neglijarea actualizării software-ului poate face sistemele informatice susceptibile la acțiunile hackerilor care ar putea încerca să infecteze computerele cu noi viruși și worms. De asemenea, poate produce consecințe grave pentru computerele dvs. Nu numai că defectele de securitate nerezolvate vor face sistemul mai puțin sigur, dar sunt și motivul pentru care majoritatea virușilor au atât de mult succes.

O politică de livrare a actualizărilor software este o politică dezvoltată de organizații care definesc cronologii și metode pentru evaluarea și livrarea actualizărilor software legate de securitate. Această politică se concentrează pe livrarea imediată a actualizărilor de securitate, într-un interval de timp restricționat (constrângere) pentru a minimiza fereastra de vulnerabilitate, dacă constrângerea permite acest lucru. Organizațiile pot adopta o abordare mai strategică, în funcție de constrângerile legate de resurse. Soluțiile inovatoare ar putea include, de exemplu, sisteme peer-to-peer bazate pe tehnologia blockchain și rețele suprapuse la scară largă, pentru a permite distribuirea extrem de eficientă și rapidă a actualizărilor de securitate către rețele largi de utilizatori finali (Mugarza, Flores, & Montero, 2020). Abordarea este de a descompune diferite categorii de patch-uri și termenele asociate acestora pentru

evaluare și livrare, pentru a se asigura că actualizările, la diferite niveluri, sunt evaluate în conformitate cu nevoile, costurile și riscurile asociate, înainte de implementare.

Iată câteva sugestii de actualizare a software-rilor potrivite pentru implementarea în organizații[1]:

- **Instalare în timp util:** Instalarea la timp a actualizărilor de securitate vă poate ajuta să vă protejați sistemele împotriva vulnerabilităților și amenințărilor.
- **Comunicare clară:** Utilizatorii sunt adesea rezistenți la actualizări, deoarece nu înțeleg de ce au nevoie de ele. Este important să comunicați de ce actualizarea este importantă și că nu este doar un patch aleatoriu furnizat de furnizor. De asemenea, este benefic să menționați în informările dvs. că unele actualizări sunt patch-uri pentru găurile de securitate care pot fi deja exploatate.
- **Minimizați perturbarea:** Activați instalări sau configurații silențioase în sistem, ceea ce ar facilita aplicarea actualizărilor. O altă modalitate de a minimiza întreruperile este distribuirea și implementarea actualizărilor în afara orelor de vârf.
- **Educarea utilizatorilor:** educarea utilizatorilor finali cu privire la importanța actualizărilor software în menținerea securității și funcționalității sistemului pentru a promova un comportament proactiv de actualizare.
- **Proceduri de testare:** Îmbunătățiți procedurile de testare pentru a vă asigura că actualizările sunt testate riguros pentru compatibilitate și riscuri potențiale înainte de implementare.
- **Diferențiați actualizările:** Distingeți actualizările de securitate de actualizările de funcționalități, astfel încât utilizatorii să înțeleagă valoarea fiecărui tip de actualizare și să le prioritizeze în consecință.
- **Actualizări cumulative:** Luați în considerare implicațiile actualizărilor cumulative și încurajați utilizatorul să instaleze corecțiile critice de securitate.

1.4 Protecție antivirus: Protejarea integrității sistemului

Potrivit Rohith și Kaur (2021), software-ul anti-virus este un program specializat care protejează sistemul de operare de viruși, spyware, atacuri hacker și alte accese neautorizate la computer pentru a preveni furtul de date personale valoroase, sau controlul neautorizat al computerului de către o altă aplicație de calculator (freeware, shareware și comercială). Software-ul antivirus este utilizat pentru a detecta virușii de calculator care pot implica fișiere de computer, programe de aplicații și sistemele de operare ale computerului. Din acest motiv, poate fi, de asemenea, configurat pentru a efectua revizuiri regulate ale

[1] (compiled from (Mathur, Malkin, Harbach, Péer, & Egelman, 2018), (Di Tizio, Armellini, & Massacci, 2022), (Vaniea, Rader, & Wash, 2014))

fișierelor și memoriei computerului, pentru a detecta orice semnătură de virus cunoscută, prevenind astfel posibila contagiune a sistemului informatic și a fișierelor sale. Este important să actualizați în mod regulat software-ul antivirus cu cele mai recente definiții și semnături de viruși, deoarece noi viruși și variații continuă să apară în mod regulat. Prin detectarea celor mai recente amenințări cu viruși, actualizarea software-ului antivirus oferă o apărare robustă împotriva evoluției constante a amenințărilor informatice pe măsură ce funcționează (Naie & Teymournejad, 2012).

Câteva indicii sunt asociate cu prezența virușilor pe computer, o parte dintre acestea fiind detaliate mai jos. Fiecare dintre aceste indicii pot indica posibile probleme cu virușii. De aceea, este important să scanați sistemul folosind un software antivirus cât mai curând posibil (Kumar, 2008):

- Computer mai lent
- Sarcinile de bază durează mai mult
- Blocări și erori
- Activitate constantă pe disc
- Utilizarea excesivă a procesorului
- Navigarea pe Internet este mult mai lentă decât înainte
- Aplicațiile nu pornesc
- Ferestre pop-up și mesaje nesolicitate cu conținut pentru adulți
- Deschiderea și închiderea unității CD-ROM

Dacă vă confruntați cu una sau mai multe dintre aceste situații în mod neașteptat, contactați administratorul IT sau efectuați verificările antivirus necesare. Este important să rețineți că instalarea unui antivirus pe toate sistemele este crucială, chiar dacă nu este cel mai bun. Acest lucru ajută la îngreunarea eforturilor atacatorilor care încearcă să compromită securitatea unui sistem (Min & Varadharajan, 2015). Mergând mai departe, Ncube & Maiden (2004) oferă informații valoroase despre provocări și considerente de investigat în timpul selecției software-ului antivirus pentru o organizație:

1. Utilizați un chestionar împreună cu alte tehnici de obținere a informației.

2. Asigurați-vă că întrebările sunt scurte și că vor asigura primirea de răspunsuri bune de la furnizori.

3. Solicitați documentația cu răspunsurile la chestionar, astfel încât să poată fi potrivită bine descrierea produsului cu produsul real.

4. Definiți clar ceea ce spuneți în produs și cât de departe veți testa vă va ajuta să definiți mai bine cazul de testare.

5. Înțelegeți că timpul pentru selectarea software-ului dorit este limitat și este de dorit să ofere șabloane de descriere a procesului pentru a fi mai rapizi în diferite ocazii.

6. Fiți conștienți că nu puteți testa totul. Unele cerințe pot avea restricții.

1.5 Copiile de rezervă ale datelor: un scut împotriva pierderii acestora

Deși neprevăzute, evenimentele neașteptate și incidentele cibernetice sunt capabile să provoace daune semnificative datelor unei organizații. Aici intră în discuție copiile de rezervă ale datelor. Copiile de rezervă ale datelor sunt o componentă critică a securității cibernetice și a menținerii unui mediu digital sigur. Copiile de rezervă ale datelor pot fi un instrument excelent pentru organizații în cazul breșelor de securitate. Împreună cu protecția datelor împotriva pierderilor, sistemele de backup oferă posibilitatea de a restabili versiunile anterioare ale fișierelor, astfel încât istoricul fișierelor să fie protejat. Majoritatea instrumentelor de backup pot păstra mai multe instanțe ale aceluiași fișier în mai multe formate, fiecare dintre ele fiind asociată cu o perioadă de timp. De asemenea, arhivarea și criptarea sunt caracteristici comune ale aproape tuturor sistemelor de rezervă. Arhivarea ajută utilizatorii să transfere fișiere într-o rețea sau pe Internet atunci când le partajează (Sampaio & Bernardino, 2015).

Tehnicile sistemelor de backup de date implică backup complet care realizează o copie completă a tuturor datelor, backup diferențial care stochează modificările de date de la ultima copie de rezervă completă și backup incremental care salvează doar porțiunile de date care s-au schimbat de la efectuarea copiei de rezervă anterioare (Nadee & Somwang, 2021). Fiecare metodă produce consecințe diferite și adecvare pentru operațiunile de rezervă. Copiile de rezervă fiabile sunt demne de remarcat, deoarece unele date sunt de neprețuit, iar recrearea suplimentară consumă timp/ bani (Traeger, Joukov, Sipek, & Zadok, 2006). Datele de rezervă nu sunt doar pentru a salva pierderile de date, ci și pentru a restabili o versiune veche (Sampaio & Bernardino, 2015). Această funcționalitate dublă este importantă atât pentru recuperarea datelor, cât și pentru respectarea anumitor standarde legale. Iată câteva dintre cele mai bune practici pentru backupul firmelor mici (Rock, 2023):

Strategia de protecție a datelor: Companiile mici trebuie să elaboreze un plan detaliat pentru protecția datelor, care va face parte din PCA (Planul de continuitate a afacerii) sau PRD (Planul de recuperare în caz de dezastru).

Soluții de backup: Companiile nu ar trebui să utilizeze soluții simple de backup, ci mai degrabă ar trebui să aleagă câteva soluții robuste BC/ DR (Business Continuity/ Disaster Recovery), care garantează o întrerupere operațională minimă.

Frecvența și stocarea backup-ului: Copiile de rezervă regulate sunt esențiale, iar soluțiile moderne de backup fac copii de rezervă frecvente. Este recomandat să aveți protecție hibridă de rezervă, care stochează date atât on site, cât și în cloud.

Securitate și conformitate: Este important să protejați copiile de rezervă împotriva atacurilor cibernetice și, de asemenea, să respectați politicile de păstrare a datelor. Criptarea copiilor de rezervă în tranzit și în repaus ar fi o securitate suplimentară.

Date de rezervă pe dispozitive securizate: configurați dispozitivele de backup pentru comunicarea de ieșire numai într-o rețea locală securizată. Această abordare vă va ajuta să împiedicați un infractor cibernetic să preia controlul asupra copiilor de rezervă.

Backup de date pe dispozitive separate: Asigurați-vă că păstrați dispozitivele de backup separate de rețeaua locală pentru a evita ca backupurile să fie afectate atunci când apare un ransomware în rețeaua locală. Unul dintre avantajele copierii de rezervă a datelor în cloud este că se poate face din orice loc conectat, departe de birourile principale ale organizației.

Utilizați backupuri criptate: utilizați stocarea și transmiterea criptate pentru a proteja datele critice împotriva accesului neautorizat, a manipulării frauduloase și a corupției.

Faceți o copie de rezervă a tuturor datelor endpoint utilizând software-ul de recuperare: O sursă foarte importantă de pierdere a datelor este laptopurile/desktopurile pierdute, furate sau corupte. Drept rezultat, incapacitatea dvs. de a face backup sau de a restabili datele pierdute. Știind că dispozitivele de backup iau forma desktopurilor și serverelor, selectați întotdeauna soluții de recuperare pentru a proteja toate datele de pe orice computer și selectați backup-ul punctului final în consecință.

1.6 Protecție împotriva codurilor rău-intenționate: să înțelegem soluțiile Anti-Malware

Executabilele rău intenționate sunt programe neautorizate create pentru a infesta sau deteriora un sistem informatic, ceea ce constituie un mare pericol pentru securitatea computerului (Ye, Wang, Lİ, & Ye, 2007). Utilizatorii sunt, de obicei, victime ale software-ului rău intenționat fără ca măcar să știe. Programul rulează în fundal pe computerul unui utilizator fără știrea acestuia și execută acțiuni precum furtul de informații, viruși care vă vor șterge dispozitivele curate sau troieni care vă pot șterge sau nu fișierele. Spyware, viruși, worms, troieni, ransomware și adware sunt versiunile comune ale malware-ului. Fiecare organizație ar trebui să-și facă backup pentru sistemele lor mai mult de o dată pe zi și să utilizeze o soluție completă anti-malware. Mai mulți factori trebuie luați în considerare atunci când alegeți software anti-malware pentru o organizație, pentru a vă asigura că soluția se potrivește nevoilor sau obiectivelor organizației (Alharbi, Alzahrani, Asseri, & Taramisi, 2020):

Funcționalități de securitate: Accesul în timp real, protecția firewall și detectarea intruziunilor sunt funcționalități cheie de securitate care trebuie incluse într-un program anti-malware. Aceste caracteristici sunt vitale pentru gestionarea eficientă a amenințărilor și pentru a vă asigura că nu există amenințări care nu au fost luat în considerare.

Funcționalități operaționale: Funcționalitățile operaționale ale software-ului anti-malware pe care ar trebui să le aveți în vedere includ: cât de ușor este să implementați și să utilizați software-ul, ce posibilități de gestionare are software-ul și modul în care se va integra cu sistemele existente.

Eficiență: Evaluați eficiența software-ului anti-malware în ceea ce privește identificarea și eliminarea software-ului dăunător. Căutați soluții care au un procent ridicat de detecție de până la 100% și un procent minim fals pozitiv.

Scalabilitate: Alegeți o soluție care se poate adapta nevoilor organizației pe măsură ce aceasta crește. Asigurați-vă că soluția software antimalware poate gestiona nevoile curente ale organizației dvs. și poate răspunde nevoilor viitoare.

Verificați reputația furnizorului: O bună reputație este esențială în industria software, dar este una dintre cele mai valoroase calități ale oricărui furnizor de software. Căutați furnizori anti-malware care au o experiență îndelungată ca furnizori de soluții de securitate de înaltă calitate. Întrebarea pe care trebuie să o aveți în vedere în realizarea selecției soluției: A fost recunoscută de organizații independente de testare?

Cost: Primul lucru de luat în considerare este prețul software-ului anti-malware. Diferiți furnizori își oferă software-ul la diferite variante de preț și opțiuni de licențiere, deci asigurați-vă că se încadrează în bugetul vostru. Unele organizații pot clasifica acest lucru ca un factor important, în timp ce altele ar putea clasifica acest lucru ca nefiind foarte important.

Suport și actualizări: Evaluați istoricul furnizorului în ceea ce privește asistența oferită și actualizările realizate. Găsiți un furnizor care oferă actualizări regulate și asistență tehnică în cazul în care apar probleme.

Compatibilitatea este unul dintre lucrurile pe care o organizație trebuie să le bifeze dintr-o listă, deoarece niciun software nu poate fi eficient dacă aveți probleme de compatibilitate. Problemele de compatibilitate reprezintă unul dintre cele mai frecvente motive pentru care software-ul unei organizații devine ineficient.

Unitatea 2 - Cum să transformi Igiena Digitală în obișnuință într-un organizație de tip startup

Dezvoltarea unei culturi a practicilor de securitate cibernetică și Igienă Digitală în operațiunile de zi cu zi ale unui startup este crucială. Practicile de Igienă Digitală sunt similare cu cele de igienă personală: furnizează protocoalele necesare de urmat pentru a păstra datele/ informațiile personale și ale organizației în siguranță (Alkhaledi & Hawamdeh, 2023). Startup-urile, de regulă cu buget insuficient, nu își pot permite eșecurile unui incident cibernetic. Implicațiile nu se limitează doar la un impact financiar, ci includ pierderea încrederii clienților, daune reputaționale și potențiale consecințe juridice, care într-un startup ar putea însemna diferența dintre scalarea cu succes sau eșecul prematur. Multe organizații încă nu au un comportament bun de Igienă Digitală, chiar dacă s-au făcut pași pentru a se soluționa probleme de Igienă Digitală (Kalhoro, Rehman, Ponnusamy, & Shaikh, 2021).

Un comportament bun de Igienă Digitală este esențial pentru a reduce amenințările cibernetice și provocările zilnice pentru abordarea problemelor de Igienă Digitală. Această Unitate servește la conturarea și extinderea strategiilor stabilite în mod uzual pentru companiile startup pentru a crea o rutină zilnică de Igienă Digitală.

2.1. Evaluarea sănătății digitale a startup-ului propriu

Evaluarea riscurilor de securitate cibernetică reprezintă o parte esențială a planificării activității; aceasta implică identificarea, evaluarea și estimarea riscurilor pentru resursele și operațiunile digitale ale unei organizații. Metoda de evaluare a riscurilor de securitate cibernetică aplicată permite organizației să își evalueze nivelul de securitate, să atribuie valoare informațiilor și sistemelor sale, să estimeze eficiența infrastructurii și activităților sale actuale de securitate și, de asemenea, să estimeze amploarea daunelor care ar apărea dacă riscurile specifice se materializează. Prin prioritizarea riscurilor identificate, organizațiile pot aloca în mod eficient resurse pentru a-și consolida apărarea și pentru a asigura continuitatea activității.

Numeroase studii oferă constatări valoroase cu privire la diferitele aspecte ale evaluării riscurilor de securitate cibernetică, care pot fi utile într-o organizație. Chavez și Ve Diğerleri (2020) indică, de asemenea, evaluarea nevoii de informație ca fiind una dintre principalele etape în gestionarea eficace a abaterilor în IMM-uri, prin utilizarea instrumentelor digitale. Selectarea tipurilor de informații care trebuie colectate pentru realizarea procedurilor și nivelul de complexitate al datelor va contribui la minimizarea riscului de integrare a sistemelor digitale. Elmarady și Rahouma (2021) au rezumat procesul de evaluare a riscurilor în domeniul securității cibernetice a aviației, dar aceste practici pot fi utilizate ca un cadru general în evaluarea riscurilor în IMM-uri:

1. Identificați sistemele care au nevoie de protecție. Înțelegând scopul cu care sistemele au fost programate să facă ceva, identificarea potențialelor amenințări la adresa acestor sisteme va fi mai facilă.

• Recunoașteți amenințările potențiale prin înțelegerea sistemelor.

• Definiți limitele sistemelor care urmează să fie evaluate și descrieți-le.

2. Enumerați toate lucrurile care s-ar putea întâmpla, pentru a provoca pierderi sau daune sistemului. Înțelegeți ce ar putea determina direct sau indirect neîndeplinirea unui obiectiv de securitate și care este diferența dintre o amenințare și o vulnerabilitate.

• Determinați scenarii care ar putea dăuna sistemului, direct sau indirect.

• Realizați evaluarea amenințărilor care pot afecta integritatea, confidențialitatea și disponibilitatea sistemului.

3. Evaluați probabilitatea și impactul amenințărilor. Pentru evaluarea nivelului în care o amenințare poate fi concretizată, trebuie abordați mulți factori.

• Evaluați probabilitatea amenințărilor.

• Evaluați impactul potențial al amenințărilor asupra siguranței, eficienței, economiei, politicii și încrederii publice.

4. Determinați nivelurile de risc. Evaluați nivelurile de risc.

• Analizați profilul de risc utilizând probabilitatea, evaluarea vulnerabilității și impactul amenințării.

• Transformați nivelurile de risc în termeni calitativi și determinați nivelul de tolerabilitate la risc.

• Clasificați nivelurile de risc utilizând o metodologie standardizată.

Implementați proceduri necesare pentru a reduce riscurile la niveluri acceptabile. Urmând acești pași, organizațiile pot evalua în mod eficient riscurile de securitate cibernetică, pot identifica amenințările și pot implementa politici pentru protejarea sistemelor critice.

2.2. Implementarea unei culturi a Igienei Digitale

Cultura Igienei Digitale, dezvoltarea unui ecosistem digital în expansiune, trebuie integrate într-o organizație de la crearea acesteia. Este un demers ce ar trebui implementat de sus în jos, de către Management. Nu este suficient să se discute despre bunăstarea digitală, ci trebuie în primul rând să fie practicată de către top-management. Primul pas îl reprezintă elaborarea de politici și proceduri. Liderii ar trebui să dezvolte și să promoveze o politică complexă care să reglementeze gestionarea datelor și să sporească securitatea. Sesiuni frecvente de training sunt foarte necesare. Ar trebui implementat un program regulat de conștientizare a angajaților cu privire la modul în care pot respecta regulile de siguranță

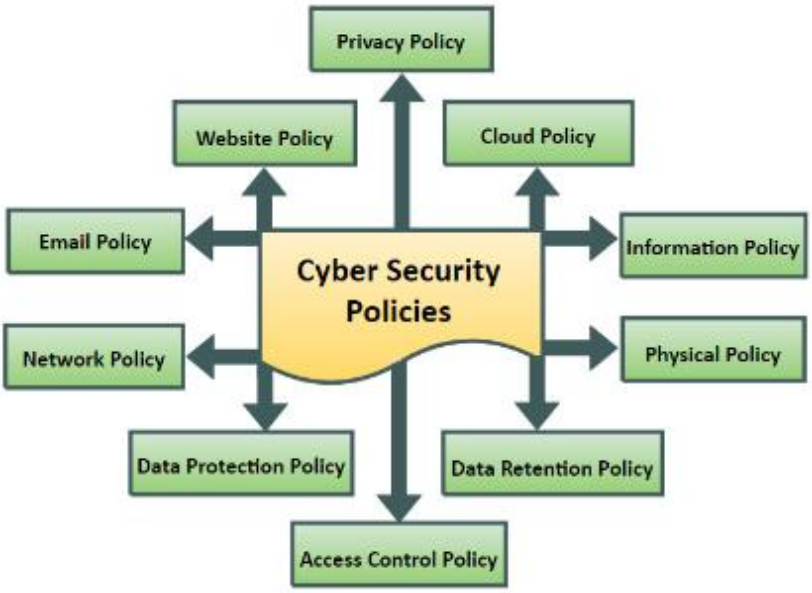
și a fi la curent cu cele mai noi practici de securitate digitală. Comunicarea deschisă este extrem de importantă. Este foarte important să existe o cultură transparentă într-o organizație în care angajații se simt confortabil să comunice, își pot exprima preocupările și, de asemenea, pot raporta dacă găsesc ceva suspect care ar putea cauza probleme de securitate. Acesta este singurul mod în care putem asigura o cultură pentru a menține igiena și securitatea digitală.

2.2.1. Elaborarea politicilor

Existența unei politici puternice de securitate cibernetică este foarte importantă pentru întreprinderile mici și mijlocii (IMM-uri), dar și alte tipuri de organizații precum startup-urile pentru a-și securiza resursele digitale și pentru a asigura continuitatea operațională. Cercetările au arătat că IMM-urile, la fel ca și în cazul startup-urilor, se confruntă cu mai multe provocări, inclusiv lipsa bugetului, lipsa specialiștilor și creșterea amenințărilor cibernetice (Neri, Niccolini, & Martino, 2023). Prin urmare, IMM-urile, precum și startup-urile trebuie să își îmbunătățească gradul de conștientizare și pregătire cibernetică. Implementarea măsurilor de securitate cibernetică poate, de asemenea, să reducă semnificativ încălcarea datelor și să îmbunătățească securitatea proceselor interne, pe lângă construirea unui sistem fiabil cu o capacitate suficientă de procesare a informațiilor (Hasani, O'Reilly, Dehghantanha, Rezania, & Levallet, 2023). În plus, reziliența IMM-urilor și a startup-urilor la atacurile cibernetice ar putea fi îmbunătățită prin politicile lor de securitate cibernetică. Punerea în aplicare a unei abordări holistice a rezilienței cibernetice ar putea îmbunătăți capacitatea MIMM-urilor și a startup-urilor de a anticipa, detecta, rezista, recupera și evolua în urma unui atac cibernetic (Carias, Borges, Labaka, Arrizabalaga, & Hernantes, 2020).

Companiile ar trebui să ia în considerare diferite domenii atunci când elaborează politici de securitate cibernetică și să producă politici de securitate cibernetică specifice domeniului de activitate, în funcție de nevoile lor. Pentru a-și promova politicile și practicile de securitate cibernetică, asociațiile pot utiliza domeniile pentru a dezvolta taxonomia politicilor de securitate cibernetică. Componentele taxonomiei politicilor de securitate cibernetică menționate de Mishra, Alzoubi, Gill, & Anwar (2022) sunt ilustrate în figura 2:

Figura 2: Taxonomia politicilor de securitate cibernetică

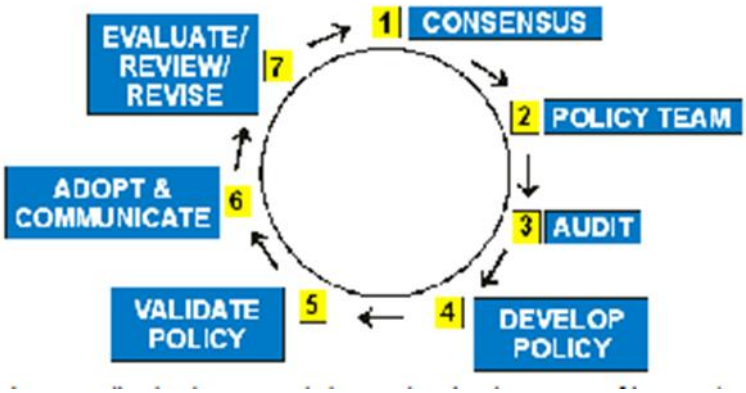


Sursa: (Mishra, Alzoubi, Gill, & Anwar, 2022)

1. Politica de confidențialitate: Se concentrează pe protejarea datelor personale sensibile și asigurarea respectării reglementărilor privind protecția datelor.
2. Securitatea site-ului web: implică securizarea site-urilor web împotriva amenințărilor și vulnerabilităților cibernetice pentru a proteja datele utilizatorilor.
3. Cloud Computing Security: Abordează măsurile de securitate pentru serviciile bazate pe cloud pentru a proteja datele stocate în cloud.
4. Securitatea e-mailului: Se concentrează pe securizarea comunicațiilor prin e-mail și prevenirea amenințărilor cibernetice bazate pe e-mail.
5. Securitate fizică: implică securizarea accesului fizic la infrastructura IT și la resursele critice pentru a preveni accesul neautorizat.
6. Securitatea rețelei: Se concentrează pe protejarea rețelelor de calculatoare împotriva amenințărilor cibernetice și a accesului neautorizat.
7. Securitatea informațiilor: cuprinde măsuri de protejare a informațiilor sensibile.
8. Controlul accesului: Implică gestionarea accesului utilizatorilor la sisteme și date pentru a preveni accesul neautorizat.
9. Păstrarea datelor: abordează politicile pentru stocarea și gestionarea datelor pe tot parcursul ciclului lor de viață.
10. Protecția datelor: Se concentrează pe protejarea datelor împotriva pierderii, furtului sau accesului neautorizat prin criptare și controale de securitate.

Odată ce cunoașteți deficiențele și obiectivele, puteți proiecta politicile de securitate cibernetică pentru a acoperi aceste domenii. Un cadru util pentru elaborarea procedurilor creat de Lubua și Pretorius (2019) este prezentat în Figura 3 . Ciclul de dezvoltare a procedurilor include recunoașterea problemelor care vor necesita dezvoltarea unui anumit tip de procedură, formarea unei echipe de experți pentru elaborare sa, discuții cu stakeholderii, validarea acesteia, adoptarea procedurii cu fiecare rezoluție valoroasă, gestionarea procedurii, actualizare ca urmare a evoluției și feedbcak-ului. De-a lungul procesului, este important să existe implicarea stakehoderilor, obținând contribuții de la diverse grupuri de oameni. Procedura trebuie, de asemenea, să fie formalizată, asigurându-vă că este în conformitate cu obiectivele organizaționale și cu oricare dintre cerințele legii. Procedurile trebuie revizuite în mod regulat, actualizându-le atunci când sunt depășite. Ar trebui să existe revizuiri și actualizări periodice. În consecință, politicile vor provoca și, de asemenea, vor opera schimbări de mediu într-o organizație sau într-un anumit context.

Figura 3: Etapele dezvoltării procedurilor



Sursa: (Lubua & Pretorius, 2019)

2.2.2. Formarea periodică

Un aspect esențial în educarea angajaților cu privire la cele mai bune practici în Igiena Digitală îl reprezintă examinarea numeroșilor factori care le influențează comportamentul și cunoștințele. Într-un studiu recent realizat de Cain, Edwards, și Still (2018), se indică faptul că utilizatorii nu sunt conștienți adesea de acțiunile cheie pe care ar trebui să le întreprindă și de impactul acestora, influențându-le astfel comportamentele. Majoritatea utilizatorilor nu înțeleg exact ce ar însemna să urmeze cele mai bune practici de securitate atunci când nu sunt conștienți de riscurile implicate. Un număr semnificativ de utilizatori pot fi, de asemenea, conștienți de riscuri, dar încă nu pot lua măsurile de precauție adecvate pentru a înțelege mai bine conceptul de securitate. Un alt studiu realizat de Neigel, Claypoole, Waldfogle, Acharya și Hancock (2020) indică factori precum factorii umani care contribuie la încălcările și riscurile cibernetice. Practicile

slabe de Igienă Digitală, lipsa de conștientizare, prejudecățile comportamentale, lacunele educaționale și formarea inadecvată influențează semnificativ factorii umani. Educația și conștientizarea pot reduce vulnerabilitatea într-o mare măsură și, astfel, pot spori și reziliența cibernetică.

Instruirea angajaților în domeniul securității cibernetice este esențială, astfel încât organizațiile să poată adopta în mod proactiv o politcă de protejare a informațiilor. Formarea angajaților nu doar pregătește angajații, ci și crește gradul de conștientizare în rândul tuturor angajaților cu privire la tipurile de amenințări cibernetice existente, care ar putea fi consecințele unui atac reușit din partea unui infractor cibernetic și cum să îl contracareze dacă ar putea destabiliza o organizație. Organizația trebuie să-și instruiască toți angajații pentru a fi bine pregătiți cu privire la securitatea cibernetică și pentru a explica orice amenințare la adresa resurselor valoroase ale companiei (Singh, Mohanty, Swagatika, & Kumar, 2020).

Iată câteva dintre cele mai bune practici pentru instruirea în domeniul securității cibernetice (Mughal, 2019) :

- Instruire regulată: Continuați să oferiți pregătire utilizatorilor finali ai organizației privind securitatea cibernetică, pentru a-i menține informați și actualizați cu privire la noile amenințări care apar în cadrul ariei responsabilităților lor.
- Conținut adaptat sau personalizat: Utilizați întotdeauna conținut de instruire personalizat sau adaptat, care se bazează pe riscul dispozitivului IoT și pe rolul utilizatorului final.
- Învățare interactivă: Este important să știți ce îi interesează pe utilizatorii finali și care este tiparul lor de învățare cu privire la subiect, să fie realizate activități tip workshop în care să se simuleze diferite situații și modalități de răspuns. Astfel se asigură interactivitatea și implicarea cursanților.
- Comunicare clară: Comunicați întotdeauna procedura privind securitatea digitală, limitările IoT, cele mai bune practici de urmat și asigurați-vă că utilizatorii le cunosc.
- Consolidare și memento-uri: Continuați să le reamintiți utilizatorilor finali procedurile și urmăriți nivelul de conștientizare în rândul acestora.
- Stimulente și recompense: Asigurați și încurajați bunele practici de securitate cibernetică prin recompense și stimulente care încurajează utilizatorii finali să finalizeze instruirea sau să raporteze incidentele.
- Evaluare și feedback: Monitorizați comportamentul utilizatorului și modul în care funcționează Responsabilul de program dacă i s-a raportat o situație.

2.2.3. Cultura organizațională

Cum poate fi aplicat conceptul de pregătire culturală la instruirea privind securitatea cibernetică a propriei organizații? Cercetările au arătat că organizațiile cu o cultură puternică în materie de securitate cibernetică sunt mai bine pregătite să facă față amenințărilor cibernetice (Berlilana, Noparumpa, Ruangkanjanases, Hariguna, & Sarmini, 2021). Cultura securității cibernetice reprezintă un element integrant în cultura generală a organizației, care modelează cadrele de referință de gestionare a riscurilor, guvernanța, politicile și comportamentele angajaților legate de securitatea cibernetică (AL-Nuaimi, 2024). Mai mult, organizațiile pot promova respectarea de către angajați a politicilor de securitate a informațiilor prin implicarea activă a managementului și prin promovarea de către aceasta a inițiativelor de securitate, comunicarea eficientă, alături de implicarea activă a angajaților (Hu, Dinev, Hart, & Cooke, 2012). O cultură comună de securitate îi ajută pe toți angajații, indiferent de departament sau de rolul postului, să înțeleagă riscurile amenințărilor cibernetice. Acest lucru ajută la o mai bună aliniere a strategiilor lor de diminuare a riscurilor de securitate cibernetică (Fritzvold, 2017).

Cadrul Tehnologie-Organizație-Mediu (TOE), dezvoltat de Tornatzky și Fleischer (1990), este un cadru cuprinzător care oferă o bază pentru ca organizațiile să poată alege din varietatea de produse și servicii ale sistemelor informatice (IS) și tehnologiei informației (IT) (Gangwar, Date, & Ramaswamy, 2015). Acest cadru reprezintă nu numai aspectul tehnic al inovației, ci și perspectiva organizațională și de mediu pentru a explica și examina adoptarea unei tehnologii (Rahayu & Day, 2015). În consecință, cadrul TOE cuprinde aceste trei dimensiuni pentru a ilustra imaginea de ansamblu a factorilor care influențează adoptarea inovațiilor în organizații. Conform (Hasan, Ali, Kurnia, & Thurasamy, 2021), factorii cheie care influențează pregătirea securității cibernetice în organizațiile bazate pe cadrul TOE sunt:

Factorii tehnologici

Maturitatea infrastructurii IT a unei organizații joacă un rol semnificativ în îmbunătățirea pregătirii acesteia de a contracara atacurile cibernetice. O infrastructură IT matură, care dispune de resursele necesare - experți, dispozitive IT și aplicații software pentru utilizatori - poate duce la îmbunătățirea pregătirii.

Factorii organizaționali

Sprijinul managementului superior, structura și cultura organizațională sunt factori importanți care stimulează pregătirea împotriva atacurilor cibernetice. În special, sprijinului din partea managementului superior are un impact semnificativ asupra instruirii.

Factorii de mediu

Relațiile cu furnizorii/ partenerii, reglementările guvernamentale și politicile din industrie sunt condiții externe de mediu care contribuie pozitiv la creșterea pregătirii organizației pentru a contracara atacurile cibernetice.

Dezvoltarea unei culturi de securitate cibernetică este un proces complex care ia în considerare cultura organizațională, subculturile și cadrele de referință. Cultura organizațională a fost identificată ca un factor esențial în modelarea culturilor de securitate, iar cultura de securitate a fost definită ca o subcultură în cadrul unei organizații. Pentru a stabili o cultură de securitate integrantă, organizația poate explora cultura prin dimensiuni precum artefactele și propune valori, ipoteze comune, cunoștințe organizaționale și practicile operaționale necesare (Uchendu, Nurse, Bada, & Furnell, 2021).

Unitatea 1 și Unitatea 2 pe scurt: Obiceiuri zilnice pentru o Igienă Digitală mai bună

O cultură puternică de Igienă Digitală este o necesitate în ecosistemul în continuă dezvoltare al startup-urilor. Implementată de management de sus în jos, această cultură subliniază importanța securității cibernetice și a protecției datelor. Pentru a facilita promovarea acestei culturi, startup-urile trebuie să implementeze copii de rezervă regulate cu protecție hibridă, prin care datele sunt stocate atât on-site, cât și în cloud. Acest lucru va ajuta la protecția împotriva atacurilor cibernetice și a defecțiunilor sistemului, iar datele vor fi în siguranță în orice moment. Copiile de rezervă criptate sunt, de asemenea, de o importanță capitală, în special pentru industrii precum asistența medicală, unde conformitatea cu protecția datelor nu este negociabilă.

Este esențial să implementați software anti-malware care oferă o suită cuprinzătoare de caracteristici, inclusiv scanarea în timp real, monitorizarea comportamentului, protecția e-mailului și filtrarea web pentru a proteja sistemele împotriva infectării cu software rău intenționat. Pe de altă parte, startup-urile ar trebui să efectueze evaluări proactive ale riscurilor de securitate cibernetică în mod regulat pentru a determina posibilele amenințări și pentru a evalua probabilitatea și impactul acestora, precum și nivelurile de risc. Evaluările vor indica punerea în aplicare a unor măsuri eficace de diminuare a riscurilor pentru a proteja sistemele critice.

Dezvoltarea unor politici și protocoale cuprinzătoare de gestionare a datelor pentru a permite manipularea în siguranță a acestora este o prioritate. Acestea trebuie să descrie politicile și procedurile pentru cele mai bune practici în materie de protecție a datelor, comunicare securizată și o bună Igienă Digitală. Personalul trebuie să fie mai bine informat cu privire la amenințările digitale și la ceea ce poate face pentru a contribui la prevenirea acestora. Acest lucru va ține personalul la curent cu cele mai recente amenințări și măsuri de securitate.

Comunicarea deschisă din punct de vedere organizațional, care permite angajaților să comunice cu ușurință preocupările legate de securitate, să raporteze activitățile suspecte și să discute despre potențialele amenințări, este vitală pentru securizarea mediului. Existența unor bune practici cotidiene de Igienă cibernetică, cum ar fi crearea de parole puternice, menținerea patch-urilor software, criptarea datelor și utilizarea canalelor de comunicare securizate trebuie să devină un obicei pentru angajați.

Un alt factor cost-eficiență de luat în considerare îl reprezintă analizarea diferitelor soluții anti-malware, costul, suportul tehnic, actualizările și compatibilitatea cu bugetul și modul în care operați. Elemente menționate anterior nu trebuie tratate ca suplimente. Startup-urile trebuie să fie în siguranță online, să-și protejeze resursele și să construiască o relație de încredere cu clienții și partenerii lor. Drept urmare Igiena Digitală și securitatea cibernetică trebuie să facă parte din ADN-ul startup-urilor. Startup-urile trebuie să combine mentenanța cibernetică și Igiena Digitală pe tot parcursul activității lor operaționale zilnice. Aceasta este singura modalitate concretă de a spori securitatea online a startup-urilor, făcându-le astfel rezistente cibernetic. Putem face o paralelă între igiena cibernetică și igiena dentară, practicarea igienei cibernetice fiind similară spălatului pe dinți sau, în acest context, cu utilizarea unor practici digitale sigure. Mai departe, putem echivala respectarea regulilor de securitate cibernetică cu folosirea apei de gură. Este important ca într-un startup să existe clar definite politici de Igienă Digitală și de securitate cibernetică, care să coexiste și să fie respectate în egală măsură.

Unitatea 3 - Integrarea Igienei Digitale: Studiu de caz și un exemplu de bune practici din cadrul startup-urilor

Cele mai bune practici: Instrumente de top de Igienă Digitală pentru startup-uri

Context: În această eră digitală, întreprinderile nou-înființate și orice afacere specială se bazează foarte mult pe tehnologie pentru activitățile lor operaționale. Astfel este foarte important să mențină Igiena Digitală pentru a se proteja de toate amenințările digitale și de încălcările de date. Fiecare startup ar trebui să dispună de anumite instrumente de Igienă Digitală care să îl ajute să își protejeze resursele digitale, astfel încât să își poată desfășura activitățile operaționale fără nicio întrerupere.

Identificarea instrumentelor de top de Igienă Dogitală: Startup-urile trebuie să își achiziționeaz o suită de instrumente de Igienă Digitală pentru a aborda diferite aspecte ale securității cibernetice. Iată o listă cu câteva instrumente utilizate de companii și organizații la scară largă:

1. **Software antivirus**: Software-ul antivirus reprezintă un sistem de controale care blochează, detectează și elimină virușii și alte programe malware dintr-un anumit software, dar și protejează datele împotriva amenințărilor online.
2. **Firewalls**: Un alt sistem de securitate îl reprezintă firewall-urile care sunt destinate dispozitivelor de securitate pe Internet, fiind concepute pentru a preveni accesul neautorizat la o rețea.
3. **Manager de parole**: ajută la crearea și menținerea unor parole puternice și unice pentru toate site-urile.
4. **Instrumente de criptare**: Criptați datele atât în repaus, cât și în tranzit, asigurându-vă că datele sensibile sunt ilizibile pentru utilizatorii neautorizați.
5. **Autentificare cu 2 factori (2FA)**: Adaugă securitate suplimentară în timpul unui proces de conectare.
6. **Rețele virtuale private (VPN)**: Oferă conexiuni sigure și criptate pentru a menține confidențialitatea și securitatea datelor în rețelele publice.
7. **Stocare securizată în cloud**: oferă un spațiu unde puteți face copii de rezervă ale fișierelor într-un loc sigur, permițând doar anumitor persoane să ajungă la acestea.

Testarea eficacității instrumentelor de Igienă digitală

În primul rând, trebuie să ne asigurăm că instrumentele alese sunt de ajutor:

1. **Verificarea compatibilității**: Asigurați-vă că instrumentele care au fost alese sunt compatibile cu sistemele actuale ale startup-ului și, în plus, nu trebuie să interfereze cu fluxurile de lucru.
2. **Evaluarea utilizabilității**: Instrumentele alese sunt implicate în realizarea sarcinilor zilnice. Astfel, trebuie să vă asigurați că nu presupun un consum suplimentar de timp și de efort.
3. **Audit de securitate:** Pentru a testa eficacitatea, instrumentele vor fi rulate în mod regulat pentru a observa dacă sunt cu adevărat sigure în fața celor mai recente forme de amenințări cibernetice.
4. **Instruire și conștientizare**: Educați echipa cu privire la importanța Igienei Digitale, eticii și utilizării responsabile a instrumentelor.

Instituirea unui culturi a Igienei Digitale

Context. Crearea unei culturi a igienei cibernetice în fiecare startup este la fel de importantă ca tehnologia în sine. Conștientizarea și pregătirea pentru securitatea cibernetică reprezintă conceptul de a promova un mediu în care fiecare angajat din fiecare startup recunoaște importanța securității cibernetice și rolul său în protejarea împotriva unei amenințări.

Crearea unei culturi a Igienei Digitale în organizația dvs:

1. **Exemplul Managementului**: Liderii direcți trebuie să conducă prin puterea exemplului și să își însușească o bună Igienă Digitală.
2. **Instruire regulată:** Instruiți angajații pe măsură ce apar noi amenințări.
3. **Proceduri clare**: Elaborați proceduri interne clare și bine definite pentru o bună Igienă Digitală.
4. **Încurajarea comunicării deschise**: Creați o cultură în care angajații sunt recompensați pentru cunoașterea sau semnalarea problemelor de Igienă Digitală.
5. **Recompensarea conformității**: Recompensați angajații care demonstrează că depășesc nivelul de bază în ceea ce privește aplicarea Igienei digitale.

Resultate și impact Rezultatele așteptate ale unei culturi a Igienei Digitale într-un startup:

- **Reducerea riscurilor de atacuri cibernetice**: O echipă bine informată reprezintă prima linie de apărare.
- **Protecția îmbunătățită a datelor**: Protejați afacerea dvs. și a clienților dvs. practicând o Igienă Digitală adecvată.
- **Respectarea reglementărilor:** Respectați reglementările privind securitatea cibernetică și evitați sancțiunile financiare și de altă natură.

Principalele idei de reținut: Startup-urile trebuie să își însușească elementele de bază corecte dacă doresc să reușească pe termen lung. Utilizarea instrumentelor de top de Igienă Digitală și încorporarea unei culturi de reziliență cibernetică în activitate sunt esențiale pentru a reduce costurile pe termen lung ale unei încălcări a datelor și pentru a accelera perioada de recuperare în cazul în care are loc un atac cibernetic.

Studiu de caz: SecureTech Startup - Adoptarea Igienei Digitale pentru securitatea cibernetică

Rezumat: este un startup fintech care a conștientizat importanța Igienei Digitale ca parte a securizării companiei lor. Acest studiu de caz vă va prezenta o schiță a diferitelor instrumente și schimbări culturale pe care le-au implementat în organizație pentru a crea un obstacol major pentru posibilele pericole asupra spațiului lor digital.

Introducere: Într-o eră de evoluție rapidă a amenințărilor cibernetice, SecureTech are o sarcină foarte dificilă de realizat, protejându-și astfel resursele digitale și datele clienților. În primele etape ale startup-ului, managementul companiei înțelege faptul că igiena digitală robustă nu este doar o necesitate pentru ei, ci și un avantaj competitiv esențial.

Analiza situației: După o evaluare inițială a securității cibernetice, compania a descoperit că are o multitudine de arii de îmbunătățit. SecureTech a îmbunătățit instrumentele utilizate în ceea ce privește Igiena Digitală și conștientizarea generală a securității cibernetice a angajaților.

Identificarea instrumentelor de Igienă Digitală: După evaluarea numeroaselor instrumente asociate cu Igiena Digitală, SecureTech a identificat o suită potrivită pentru situația lor specifică.

1. **BitDefender**: protejează toate dispozitivele împotriva diverselor amenințări.
2. **Cisco Firewalls**: monitorizează și controlează traficul de rețea.
3. **LastPass**: Manager de parole la alegere.
4. **VeraCrypt**: criptează toate datele.
5. **Duo Security**: folosit pentru autentificarea cu doi factori.
6. **NordVPN**: protejează conexiunea la distanță și munca de acces neautorizați.
7. **Dropbox Business**: stochează în siguranță copiile de rezervă și fișierele în cloud.

Dezvoltarea unei culturi a igienei digitale: conducerea SecureTech a proiectat și a introdus un program de Igienă Digitală în companie.

Angajamentul CEO-ului: Sprijinul pentru utilizarea programului la nivelul întregii companii a fost facilitat de aprobarea CEO-ul .

1. **Instruire lunară în domeniul securității cibernetice**: Au fost organizate ateliere de lucru pentru a ține echipa la curent cu cele mai recente amenințări și tendințe.

2. **Manual de Igienă Digitală:** Un set cuprinzător de politici și proceduri a fost furnizat ca Desk Drop tuturor angajaților.

3. **Campioni ai securității:** Angajații selectați au fost instruiți pentru a fi avocați ai securității cibernetice pentru departamentele respective.

4. **Recompensă și recunoaștere pentru obiceiuri sigure:** Persoanele cu o Igienă Digitală excelentă au fost recunoscute și recompensate.

Provocări și soluții. Obiecții la schimbări: adoptarea noilor instrumente, schimbări de ordin cultural în practicile de Igienă Culturală.

1. Reducerea obstacolelor: Ne-am asigurat că noile noastre seturi de instrumente digitale au sporit eficiența fiecărei echipe, în loc să le încetinim.

2. A face instruirea de securitate distractivă: Am implementat un program de instruire în domeniul securității bazat pe jocuri, care ar clasifica echipele în funcție de abilitățile lor cibernetice.

3. **Informarea angajaşilor noştri:** Am comunicat continuu progresul pe care îl făcea TeamSecureTech și IMPACTUL pe care eforturile lor de igienă digitală îl aveau asupra securității companiei lor.

Rezultate: În decurs de un an, SecureTech a raportat:

• **100% adoptarea instrumentelor de Igienă Digitală -** Instrumentele alese au fost adoptate integral de personal.

• **Reducerea cu 80% a tentativelor de phishing –** Creșterea gradului de conștientizare a personalului a permis recunoașterea și raportarea mai rapidă a e-mailurilor suspecte.

• **Îmbunătățirea poziției de conformitate –** Toate standardele de reglementare au fost îndeplinite și nu au fost aplicate amenzi.

Concluzie: Având o poziție extrem de proactivă privind igiena digitală, SecureTech și-a îmbunătățit considerabil securitatea cibernetică și a dezvoltat o cultură a vigilenței și responsabilității. Acest studiu de caz ilustrează modul în care un mediu complex de amenințări poate fi înfrânt prin intermediul unui cadru de control eficient care funcționează la unison cu transformarea culturii unei companii.

De reținut:

Selectarea instrumentului potrivit este esențială: startup-urile trebuie să caute instrumente de Igienă Digitală care să se potrivească nevoilor și fluxurilor lor de lucru specifice.

Cultura stimulează conformitatea: construirea unei culturi puternice a Igienei Digitale poate reduce riscurile de securitate cibernetică.

Este un proces de îmbunătățire: securitatea cibernetică nu este o stare, ci un proces continuu, nu este o acțiune unică și necesită actualizări periodice și activități de instruire.

Referințe

Alharbi, B., Alzahrani, H., Asseri, A., & Taramisi, K. (2020). Anti-malware efficiency evaluation framework. *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* (s. 1-4). IEEE.

Alkhaledi, R., & Hawamdeh, S. (2023). Electronic health records and cyber hygiene: a qualitative study of the awareness, knowledge, and experience of physicians in Kuwait. *Proceedings of the Association for Information Science and Technology, 60(1)*, s. 21-30.

AL-Nuaimi, M. N. (2024). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review. *Global Knowledge, Memory and Communication, 73* ((1/2)), 1-23.

Berlilana,Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. *Sustainability, 13*(24), 13761.

Blocki, J., & Liu, P. (2023). Towards a rigorous statistical analysis of empirical password datasets. *2023 IEEE Symposium on Security and Privacy (SP)*, 606-625.

Bruzgiene, R., & Jurgilas, K. (2019). Securing remote access to information systems of critical infrastructure using two-factor authentication. *Electronics, 10*(15), 1819.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications, 42*, 36-45.

Carias, J. F., Borges, M. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). a systematic approach to cyber resilience operationalization in SMEs. *IEEE Access*, *8*, s. 174200-174221.

Chavez, Z., Hauge, J. B., Bellgran, M., Gullander, P., Johansson, M., Medbo, L., & Ström, M. (2020). Digital tools and information need assessment for efficient deviation handling in SMEs. *Advances in Transdisciplinary Engineering., 13*(SPS2020), 24 - 35.

De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2013). A comparative usability study of two-factor authentication. *arXiv preprint, 1309*, 5344.

Di Tizio, G., Armellini, M., & Massacci, F. (2022). Software updates strategies: A quantitative evaluation against advanced persistent threats. *IEEE Transactions on Software Engineering, 49*(3), 1359-1373.

Elmarady, A. A., & Rahouma, K. (2021). Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. *IEEE Access, 9*, 143997-144016.

Fritzvold, E. (2017). Cyber Security in Organizations. *(Master's thesis, University of Stavanger, Norway)*.

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management, 28*(1), 107-130.

Han, W., Sun, C., Shen, C., Chang, L., & Shen, S. (2013). Dynamic combination of authentication factors based on quantified risk and benefit. *Security and Communication Networks, 7*(2), 385-396.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications, 58*, 102726.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business &Amp; Economics, 3*(5).

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660.

Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. *Proceedings of the Sigchi conference on human factors in computing system*, (s. 383-392).

Jones, C. (2022, 11 24). *Expert Insights*. https://expertinsights.com/insights/the-most-significant-password-breaches/ Dresden alındı

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting key factors of cyber hygiene behavior among software engineers: a systematic literature review. *IEEE Access*, *9*, s. 99339-99363.

Kato, K., & Klyuev, V. (2013). Strong passwords: Practical issues. *2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems(IDAACS). 2*, s. 608-613. IEEE.

Keszthely, A. (2013). About passwords. *Acta Polytechnica Hungarica*, 99-118.

Kumar, P. (2008). Computer virus prevention & anti-virus strategy. *Sahara Arts & Management Academy Series.*

Lubua, E. W., & Pretorius, P. D. (2019). Cyber-security policy framework and procedural compliance in public organizations. *Proceedings of the International Conference on Industrial Engineering and Operations Management*, (s. 1-13).

Mathur, A., Malkin, N., Harbach, M., Péer, E., & Egelman, S. (2018). Quantifying users' beliefs about software updates., (s. Proceedings 2018 Workshop on Usable Security.).

Min, B., & Varadharajan, V. (2015). Design, implementation, and evaluation of a novel anti-virus parasitic malware. *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, (s. 2127-2133).

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors, 22*(2), 538.

Mugarza, I., Flores, J. L., & Montero, J. L. (2020). Security issues and software update management in the industrial Internet of Things (IoT) era. *Sensors, 20*(24), Sensor.

Mughal, A. A. (2019). Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges. *Applied Research in Artificial Intelligence and Cloud Computing, 2*(1), 1-31.

Nadee, P., & Somwang, P. (2021). Efficient incremental data backup of unison synchronize approach. *Bulletin of Electrical Engineering and Informatics, 10*(5), 2707-2715.

Naie, H., & Teymournejad, K. (2012). Choosing the best anti-virus in the world by application of the TOPSIS method. *Life Science Journal, 9*(4).

Ncube, C., & Maiden, N. (2004). Selecting cots anti-virus software for an international bank: Some lessons learned. *Proceedings 1st MPEC Workshop.*

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*(92), 101731.

Neri, M., Niccolini, F., & Martino, L. (2023). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information &Amp; Computer Security, 32*(1), 38-52.

Pearce, M., Zeadally, S., & Hunt, R. (2010). Assessing and improving authentication confidence management. *Information Management & Computer Security, 18*(2), 124-139.

Rahayu, R., & Day, J. (2015). Rahayu, R., & Day, J. (2015). Determinant factors of e-commerce adoption by SMEs in developing country: evidence from Indonesia. *Procedia-social and behavioral sciences, 195*, 142-150.

Rock, T. (2023, 10). *Invenioit*. https://invenioit.com/continuity/10-best-practices-for-small-business-backup/ adresinden alındı

Rohith, C., & Kaur, G. (2021). A comprehensive study on malware detection and prevention techniques used by anti-virus. *2021 2nd International Conference on Intelligent Engineering and Management (iciem)* (s. 429-434). IEEE.

Sampaio, D., & Bernardino, J. (2015). Open source backup systems for SMEs. *New Contributions in Information Systems and Technologies*, 823-832.

Sampaio, D., & Bernardino, J. (2015). Open-source backup systems for SMEs. *New Contributions in Information Systems and Technologies: Volume 1*, 823-832.

Singh, D., Mohanty, N. P., Swagatika, S., & Kumar, S. (2020). Cyber-hygiene: The key concept for cyber security in cyberspace. *Test Engineering and Management*, 8145-8152.

Tellini, N., & Vargas, F. (2017). *Two-Factor Authentication: Selecting and implementing a two-factor authentication method for a digital assessment platform.*

Traeger, A., Joukov, N., Sipek, J., & Zadok, E. (2006). Using free web storage for data backup. *Proceedings of the Second ACM Workshop on Storage Security and Survivability.*

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387.

Vaniea, K. E., Rader, E., & Wash, R. (2014). Betrayed by updates: how negative experiences affect future security. *Proceedings of the SIGCHI conference on human factors in computing systems*, (s. 2671-2674).

Ye, Y., Wang, D., Lİ, T., & Ye, D. (2007). IMDS: Intelligent malware detection system. *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*, (s. 1043-1047).

Modulul 3 – Igiena Digitală în startup-uri

Unitatea 1 – Rolul Igienei Digitale în dezvoltarea și securitatea startup-urilor

La fel ca menținerea unei sănătăți fizice bune, păstrarea unei igiene digitale puternice este esențială pentru a fi mai în siguranță în mediul online. Igiena digitală ar trebui să se transforme într-o rutină pentru noi toți, atât în ceea ce privește activitatea online în interes personal, cât și profesional.

Ca start-up-uri, atunci când definiți reguli și politici interne, trebuie să includeți și reguli de Igienă Digitală și bune practici care să fie urmate de toți angajații.

Majoritatea activităților noastre profesionale se desfășoară online folosind instrumente digitale. Așadar, trebuie să fiți conștienți de riscurile posibile și să implementați politici specifice pentru a le diminua și pentru a menține o bună igienă digitală în startup-ul dvs.

Înainte de a considera implementarea unei politici de Igienă Digitală drept o sarcină formală pe care trebuie să o bifați, gândiți-vă la toate beneficiile pe care le poate aduce.

Așadar, implementarea unei politici de Igienă Digitală pentru startup-ul dvs. nu este doar ceva ce ați putea avea, ci un must-have pentru a proteja viața profesională și personală a angajaților dvs. Dacă aveți nevoie de câteva motive pentru a sublinia necesitatea practicilor de Igienă Digitală în startup-uri, să trecem în revistă câteva motive pentru care aceasta este esențială pentru o astfel de organizație.

Startup-urile sunt organizații mici, cu resurse limitate și fără infrastructura puternică de securitate a organizațiilor de mari dimensiuni. Acest lucru le face ținte atractive pentru infractorii cibernetici și mai susceptibile la amenințările cibernetice. O politică de Igienă Digitală ajută la implementarea unor măsuri eficiente de securitate și la diminuarea riscurilor posibile.

În concluzie, pentru startup-uri, o politică de Igienă Digitală este fundamentală pentru securitatea acestora, consolidarea încrederii, scalabilitate, rentabilitate și eficiență operațională. Ajută la stabilirea direcției pentru practici digitale responsabile și sigure, ceea ce este crucial pentru succesul sustenabil și dezvoltarea startup-ului în contextul digital actual.

Unitatea 2 - Beneficiile implementării practicilor de Igienă Digitală în startup-uri

Care sunt beneficiile implementării unor bune practici de Igienă Digitală?

Pe scurt, practicarea unei bune Igiene Digitale vă face prezența online sigură și sănătoasă, ținând cont de mediul de afaceri actual, care se bazează tot mai mult pe tehnologie. Așadar, beneficiile pot fi clasificate pe două niveluri:

1. **Securitate și mentenanță**
2. **Sănătate**

Să descoperim care sunt principalele beneficii!

1. **Securitate și mentenanță**

Implementarea unor politici bune de Igienă Digitală și a celor mai bune practici vă va menține în siguranță mediul digital la locul de muncă (și personal). Nu uitați să definiți regulile de mentenanță, pentru a vă asigura că toți angajații sunt conștienți de politica internă și că regulile sunt actualizate cu noile amenințări posibile.

Este recomandat să efectuați traininguri periodice de conștientizare a securității cibernetice, pentru a vă asigura că echipa dvs are cunoștințele necesare pentru a răspunde corect eventualelor noi amenințări cibernetice.

Cum putem rezuma principalele beneficii pentru startup-uri atunci când implementează și mențin bune practici de igienă digitală pentru a-și proteja securitatea în mediul digital?

- **Securitatea și respectarea confidențialității datelor**

Protecția informațiilor sensibile este esențială. Actualizarea regulată a software-ului, utilizarea de parole puternice și implementarea tehnicilor de criptare pot ajuta la protejarea datelor sensibile împotriva amenințărilor cibernetice. O bună Igienă Digitală ajută la protejarea informațiilor sensibile și previne accesul neautorizat, reducând riscul de încălcare a datelor. Respectarea reglementărilor privind protecția datelor asigură faptul că startup-ul evită problemele legale și construiește o relație de încredere cu clienții.

De asemenea, protejarea datelor financiare și ale clienților este esențială pentru startup-uri. Igiena digitală asigură tranzacții online sigure și integritatea datelor financiare.

- **Managementul reputației și construirea încrederii**

Clienții și partenerii au încredere în companiile care acordă prioritate securității digitale. Demonstrarea unui angajament față de securitatea digitală și confidențialitate poate spori reputația startup-ului și poate construi o relație de încredere cu clienții, investitorii și partenerii. De asemenea, impactul negativ al incidentelor de securitate poate fi evitat. Resursele digitale bine întreținute, inclusiv un site web ușor de utilizat și tranzacții online sigure, contribuie la o imagine profesională.

- **Conformitate și protecție juridică: îndeplinirea cerințelor de reglementare**

Multe sectoare de activitate au reglementări stricte privind protecția datelor și confidențialitatea. Respectarea reglementărilor specifice industriei și a standardelor de conformitate ajută startup-urile să evite complicațiile legale, amenzile și daunele reputaționale. Adoptarea acestor reglementări nu numai că protejează start-up-ul de consecințele legale, ci ajută și la construirea unei imagini de brand de încredere.

Auditurile și revizuirile sunt un alt aspect important. Auditarea periodică a practicilor digitale asigură faptul că startup-ul rămâne conform cu reglementările în evoluție și standardele din industrie.

- **Continuitatea operațională: reducerea timpilor morți**

Incidentele de securitate cibernetică, cum ar fi atacurile malware sau pierderea datelor, pot duce la perioade de nefuncționare semnificative. Măsurile de Igienă Digitală ajută la prevenirea și atenuarea unor astfel de incidente, asigurând operațiuni de afaceri fără întreruperi.

- **Economii de costuri: evitarea pierderilor financiare**

Recuperarea după un incident de securitate cibernetică poate fi costisitoare financiar. Copiile de rezervă periodice și metodele de stocare securizate pot preveni pierderea datelor, salvând startup-ul de costurile potențial ridicate asociate cu recuperarea informațiilor pierdute. Investiția timpurie în măsuri de securitate digitală este o abordare proactivă care ajută la prevenirea potențialelor pierderi financiare cauzate de atacurile cibernetice, cum ar fi ransomware-ul sau încălcarea datelor.

- **Inovare și creștere: stimularea inovării**

Un mediu digital sigur permite startup-urilor să se concentreze asupra inovării, fără a fi în mod constant distrase de preocupările legate de securitatea cibernetică. Acest lucru stimulează creativitatea și accelerează creșterea afacerii. Prin automatizarea sarcinilor de rutină și optimizarea fluxurilor de lucru digitale, startup-urile pot elibera timp și resurse pentru a se concentra pe inovare și inițiative strategice. O bună Igienă Digitală asigură că startup-ul este pregătit din punct de vedere tehnologic să adopte noi instrumente și tehnologii, rămânând competitiv pe piață.

- **Încrederea și loialitatea clienților: protejarea informațiilor despre clienți**

Este mai probabil ca un client să interacționeze cu companii care acordă prioritate securității informațiilor personale. Igiena Digitală generează încrederea și loialitatea clienților, contribuind la crearea de relații pe termen lung.

- **Securitatea lanțului de aprovizionare: asigurarea securității furnizorilor și partenerilor**

Bunele practici de Igienă Digitală se extind dincolo de sistemele interne ale startup-ului pentru a include comunicarea securizată și schimbul de date cu furnizorii și partenerii, asigurând un lanț de aprovizionare securizat end-to-end.

- **Adaptabilitate la amenințările emergente: fiți cu un pas înaintea amenințărilor**

Igiena Digitală implică informarea cu privire la cele mai recente amenințări la adresa securității cibernetice și implementarea măsurilor de contracarare a acestora. Această adaptabilitate este crucială în peisajul în continuă evoluție al amenințărilor cibernetice.

2. **Sănătate**

Suntem copleșiți de numeroasele tehnologii digitale și platforme online pe care ne petrecem timpul în timpul zilei. Nu trebuie să neglijăm impactul pe care îl pot avea asupra sănătății noastre mintale. Dacă în timpul programului de lucru respectăm regulile existente din organizațiile noastre, în viața personală ar trebui să avem și o bună igienă digitală. A fi atent cu timpul petrecut în fața ecranului, a evita supraexpunerea și prea multe ore pe rețelele sociale, utilizarea unui manager de parole și a autentificării cu doi factori pentru conturile dvs. vă va aduce doar siguranță.

Implementarea bunelor practici de Igienă Digitală are numai beneficii pentru productivitatea și moralul angajaților. Distragerile sunt reduse, iar angajații pot fi mai productivi atunci când nu se confruntă în mod constant cu probleme de securitate. Un mediu digital sigur promovează o atmosferă pozitivă la locul de muncă și ridică moralul.

De asemenea, putem menționa ca beneficii suplimentare ale implementării și menținerii practicilor de Igienă Digitală:

- **Flux de lucru eficient.** Organizarea corectă a resurselor și fișierelor digitale poate eficientiza procesele de lucru, permițând angajaților să găsească rapid informații și să finalizeze sarcinile mai eficient.
- **Colaborare.** Practicile de Igienă Digitală, cum ar fi utilizarea instrumentelor de colaborare și stocarea în cloud, îmbunătățesc munca în echipă prin furnizarea unei platforme centralizate pentru comunicare și partajarea fișierelor.

- **Adaptare ușoară la creștere și scalabilitate**. Implementarea de la început a soluțiilor digitale scalabile permite startup-urilor să se dezvolte fără întreruperi semnificative sau necesitatea unor revizuiri majore ale infrastructurii digitale.
- **Flexibilitate.** Menținerea unui mediu digital curat și organizat oferă flexibilitatea de a se adapta la nevoile de afaceri în schimbare și la tendințele pieței.
- **Agilitate.** Startup-urile, cunoscute pentru agilitatea lor, beneficiază de fluxuri de lucru eficiente și de colaborare permise de o politică bine implementată.

Unitatea 3 - Amenințări potențiale și consecințe ale neglijării Igienei Digitale

În martie 2023, Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) a publicat un raport amplu privind amenințările și provocările la adresa securității cibernetice pentru 2030, cu scopul de a spori gradul de conștientizare a viitoarelor amenințări și contramăsuri în rândul statelor sale membre și al părților interesate (Mattioli et al., 2023). Multe dintre amenințările identificate sunt deja relevante astăzi, iar în anii următori vor rămâne presante. În octombrie 2023, aceeași agenție a publicat un raport privind amenințările care au fost raportate în perioada iulie 2022 și iunie 2023: ENISA Threat Landscape 2023 (Lella, 2023).

Deși publicul și părțile interesate ale acestor rapoarte sunt numeroase, atât din sectorul public, cât și din cel privat, ele sunt deosebit de relevante în contextul startup-urilor. Acestea din urmă sunt deosebit de vulnerabile la amenințările cibernetice din cauza unei combinații de factori, adesea legați de structura lor, constrângerile legate de resurse și natura rapidă a mediului de afaceri. Pe măsură ce întreprinderile emergente se bazează din ce în ce mai mult pe tehnologie și platforme online pentru operațiunile lor, acestea devin mai susceptibile la atacuri cibernetice. După cum s-a subliniat anterior, consecințele potențiale asupra victimei amenințărilor cibernetice includ încălcări ale datelor, pierderi financiare, deteriorarea reputației și chiar întreruperea afacerii. Start-up-urile gestionează adesea informații sensibile, în timp ce nu dispun de infrastructura și resursele pe care le au organizațiile mai mari, ceea ce le face ținte atractive pentru infractorii cibernetici care încearcă să exploateze vulnerabilitățile.

Vulnerabilitatea startup-urilor la amenințările cibernetice poate avea, de asemenea, un impact semnificativ asupra economiei în general și asupra unor structuri publice. De exemplu, mai multe moduri în care vulnerabilitățile startup-urilor pot influența aspecte economice și societale mai largi pot include pierderi economice, pierderi de locuri de muncă și șomaj, încetinirea inovării, pierderea proprietății intelectuale, erodarea încrederii clienților, întreruperi ale lanțului de aprovizionare, ramificații juridice și de reglementare, intervenție guvernamentală sporită și chiar preocupări legate de securitatea națională. Prin urmare, startup-urile trebuie să recunoască și să crească gradul de conștientizare cu privire la toate amenințările existente și potențiale viitoare pentru a se proteja pe ele însele și societatea în general.

O înțelegere vastă a amenințărilor cibernetice și punerea în aplicare a unor măsuri de securitate solide sunt imperative pentru ca startup-urile să diminueze riscurile și să stabilească o bază solidă pentru succesul pe termen lung în domeniul digital. Pentru a contribui la creșterea gradului de conștientizare cu privire la varietatea amenințărilor cibernetice, le vom prezenta mai jos pe cele incluse în raportul "ENISA Threat Landscape 2023" (Lella, 2023).

Principalele amenințări incluse în raport sunt ransomware, malware, inginerie socială, amenințări asupra datelor, refuzul serviciului, amenințări pe internet, manipularea informațiilor și atacuri asupra lanțului de aprovizionare. Le-am definit pe scurt și apoi am inclus definițiile din raportul "ENISA Threat Landscape 2023".

1. **Ransomware.** Ransomware este un tip de software rău intenționat conceput pentru a bloca accesul la un sistem informatic sau la fișiere până când o sumă de bani sau răscumpărare este plătită atacatorului. Poate cripta fișierele, făcându-le inaccesibile victimei.
2. **Programe malware.** Malware, prescurtarea pentru software rău intenționat, este un termen folosit pentru a descrie orice software sau cod creat cu intenția de a dăuna unui sistem informatic, de a fura date sau de a perturba operațiunile normale. Acesta include diferite tipuri, cum ar fi viruși, worms și troieni.
3. **Inginerie socială.** Ingineria socială este o metodă de manipulare a indivizilor pentru a dezvălui informații sensibile sau pentru a efectua acțiuni care pot compromite securitatea. Tehnicile includ phishing, uzurparea identității și manipularea psihologică pentru a exploata comportamentul uman.
4. **Amenințări împotriva datelor.** Amenințările împotriva datelor includ acțiuni intenționate sau neintenționate care compromit confidențialitatea, integritatea sau disponibilitatea datelor. Aceasta include încălcări ale datelor, scurgeri sau orice acces neautorizat sau divulgare a informațiilor sensibile.
5. **Refuzul serviciului (DoS).** Refuzul serviciului este un atac care are ca scop perturbarea sau dezactivarea funcționării normale a unui sistem informatic, a unei rețele sau a unui serviciu, făcându-l temporar sau pe termen nelimitat indisponibil utilizatorilor. Distributed Denial of Service (DDoS) implică mai multe sisteme care coordonează atacul.
6. **Amenințări pe internet.** Amenințările pe internet se referă la întreruperi intenționate sau neintenționate ale internetului sau comunicațiilor electronice, provocând întreruperi, opriri sau cenzură. Aceste amenințări pot rezulta din diverși factori, inclusiv atacuri cibernetice, probleme tehnice sau acțiuni direcționate de guvern.
7. **Manipularea informațiilor.** Manipularea informațiilor implică eforturi intenționate și coordonate pentru a avea un impact negativ asupra valorilor, procedurilor și proceselor politice. Aceasta poate include răspândirea dezinformării, a știrilor false sau desfășurarea de activități care manipulează opinia publică sau perturbă fluxurile normale de informații.
8. **Atacuri asupra lanțului de aprovizionare.** Atacurile asupra lanțului de aprovizionare vizează relația dintre organizații și furnizorii lor. Aceste atacuri implică compromiterea securității lanțului de aprovizionare pentru a obține acces neautorizat sau influență asupra unei organizații țintă. Exemplele includ compromiterea actualizărilor software sau a componentelor hardware.

Principalele amenințări definite în raportul "ENISA Threat Landscape 2023"

„Ransomware

Potrivit raportului ENISA privind contextul amenințărilor pentru atacurile ransomware, ransomware-ul este definit ca un tip de atac în care atacatorii preiau controlul asupra activelor unei ținte și solicită o răscumpărare în schimbul revenirii disponibilității activului. Această definiție independentă de acțiune este necesară pentru a acoperi contextul amenințărilor ransomware în schimbare, prevalența tehnicilor multiple de extorcare și diferitele obiective, altele decât câștigurile financiare, ale făptașilor. Ransomware-ul a fost, încă o dată, una dintre principalele amenințări în perioada de raportare, cu mai multe incidente de profil înalt și extrem de mediatizate.

Malware

Malware-ul, denumit și cod rău intenționat și logică rău intenționată, este un termen general utilizat pentru a descrie orice software sau firmware destinat să efectueze un proces neautorizat care va avea un impact negativ asupra confidențialității, integrității sau disponibilității unui sistem.

Inginerie socială

Ingineria socială cuprinde o gamă largă de activități care încearcă să exploateze eroarea umană sau comportamentul uman cu scopul de a obține acces la informații sau servicii. Folosește diverse forme de manipulare pentru a păcăli victimele să facă greșeli sau să predea informații sensibile sau secrete. Utilizatorii pot fi ademeniți să deschidă documente, fișiere sau e-mailuri, să viziteze site-uri web sau să acorde acces la sisteme sau servicii. Deși momelile și trucurile folosite pot abuza de tehnologie, ele se bazează pe un element uman pentru a avea succes. Acest tip de amenințare constă în principal din următorii vectori de atac: phishing, spear-phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps, and scareware. În timp ce tehnicile de inginerie socială sunt adesea folosite pentru a obține acces inițial, ele pot fi, de asemenea, utilizate în etapele ulterioare într-un incident sau încălcare. Exemple notabile sunt compromiterea e-mailului de afaceri (BEC), frauda, uzurparea identității, contrafacerea și, mai recent, extorcarea.

Amenințări la adresa datelor

O încălcare a securității datelor este definită în GDPR ca orice încălcare a securității care duce la distrugerea, pierderea, modificarea sau divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod (articolul 4.12 GDPR). Din punct de vedere tehnic, amenințările împotriva datelor pot fi clasificate în principal ca încălcări ale datelor sau scurgeri de date. Deși adesea folosite ca concepte interschimbabile, ele implică concepte fundamental diferite, care se află în cea mai mare parte în modul în care se întâmplă. O încălcare a datelor este un atac cibernetic intenționat adus de un infractor cibernetic cu scopul de a obține acces neautorizat și de a obține date sensibile, confidențiale sau protejate. Cu alte cuvinte, o încălcare a datelor este un atac deliberat și puternic împotriva unui sistem sau a unei organizații cu intenția de a fura date. O scurgere de date este un eveniment (de exemplu, configurări greșite, vulnerabilități sau erori umane) care poate provoca pierderea sau expunerea neintenționată a datelor sensibile, confidențiale sau protejate (atacurile intenționate sunt uneori denumite expunere de date).

Amenințări la adresa disponibilității: Refuzul serviciului

Disponibilitatea este ținta unei multitudini de amenințări și atacuri, printre care se remarcă DDoS. DDoS vizează disponibilitatea sistemelor și a datelor și, deși nu reprezintă o amenințare nouă, joacă un rol semnificativ în domeniul amenințărilor la adresa securității cibernetice (pag. 6 -7). Atacurile apar atunci când utilizatorii unui sistem sau serviciu nu pot accesa datele, serviciile sau alte resurse relevante. Acest lucru poate fi realizat prin epuizarea serviciului și a resurselor sale sau prin supraîncărcarea componentelor infrastructurii de rețea (pag. 8).

Amenințări la adresa disponibilității: amenințări pe internet

Amenințările la adresa disponibilității internetului se referă la întreruperi intenționate sau neintenționate asupra internetului sau comunicațiilor electronice care duc la întreruperi ale internetului, întreruperi, închideri sau cenzură. Întreruperile internetului se pot datora opririlor internetului dictate de guvern, cicloanelor, cutremurelor masive, întreruperilor de curent, întreruperilor de cablu, atacurilor cibernetice, problemelor tehnice și acțiunilor militare. Aceste amenințări se diversifică și cresc, atingând un nou record în această perioadă de raportare și

provocând pierderi monetare uriașe economiilor naționale.

Manipularea informațiilor

Manipularea și interferența informațiilor străine (FIMI) descrie un model de comportament în mare parte non-ilegal care amenință sau are potențialul de a avea un impact negativ asupra valorilor, procedurilor și proceselor politice. O astfel de activitate are un caracter manipulator și se desfășoară într-o manieră intenționată și coordonată. FIMI poate fi efectuată de actori statali sau nestatali, inclusiv de împuterniciții acestora în interiorul și în afara teritoriului lor, în timp ce în acest raport studiem amenințarea, indiferent de originea acesteia.

Atacuri asupra lanțului de aprovizionare

Un atac asupra lanțului de aprovizionare vizează relația dintre organizații și furnizorii lor. Pentru prezentul raport ETL, Curtea utilizează definiția menționată în documentul ENISA intitulat Threat Landscape for Supply Chain Attacks, în care se consideră că un atac are o componentă a lanțului de aprovizionare atunci când constă într-o combinație de cel puțin două atacuri. Pentru ca un atac să fie clasificat drept atac asupra lanțului de aprovizionare, atât furnizorul, cât și clientul trebuie să fie ținte. SolarWinds a fost una dintre primele dezvăluiri ale acestui tip de atac și a arătat impactul potențial al atacurilor lanțului de aprovizionare. S-a observat că atacatorii continuă să se hrănească din această sursă pentru a-și desfășura operațiunile și pentru a câștiga un punct de sprijin în cadrul organizațiilor, pentru a beneficia de impactul pe scară largă și de baza mare de victime a unor astfel de atacuri".

Lella, I.; Tsekmezoglou, E.; Theocharidou, M.; Magonara, E.; Malatras, A.; Naydenov, R.S.; Ciobanu, C. (2023). ENISA Threat Landscape 2023. ENISA, pag. 6-8

În plus față de amenințările cibernetice definite mai sus (ransomware, malware, inginerie socială, amenințări asupra datelor, refuzul serviciului, amenințări pe internet, manipularea informațiilor și atacuri asupra lanțului de aprovizionare), startup-urile se pot confrunta cu diverse alte amenințări la adresa securității cibernetice. Câteva amenințări suplimentare de care trebuie să fiți conștienți sunt:

1. **Atacuri de phishing.** Phishingul implică utilizarea de e-mailuri, mesaje sau site-uri web înșelătoare pentru a păcăli persoanele să dezvăluie informații sensibile, cum ar fi nume de utilizator, parole sau detalii financiare. Atacurile de phishing pot fi foarte bine direcționate (spear-phishing) sau mai răspândite.
2. **Atacuri de tip man-in-the-middle (MitM).** În atacurile MitM, o entitate neautorizată interceptează și poate modifica comunicarea dintre două părți. Acest lucru poate duce la furtul de date, interceptarea sau introducerea de conținut rău intenționat în fluxul de comunicare.
3. **Exploit-uri zero-day.** Vulnerabilitățile zero-day sunt vulnerabilități software necunoscute furnizorului și care nu au fost corectate. Autorii amenințărilor pot exploata aceste vulnerabilități înainte de dezvoltarea unei remedieri, prezentând un risc pentru orice organizație care utilizează software-ul afectat.
4. **Amenințări persistente avansate (APT).** APT-urile sunt atacuri cibernetice sofisticate și direcționate, orchestrate de obicei de indivizi bine finanțați și organizați. Aceste atacuri implică adesea o infiltrare prelungită și ascunsă a unei rețele, cu scopul de a fura informații sensibile.
5. **Vulnerabilități IoT (Internet of Things).** Pe măsură ce startup-urile integrează din ce în ce mai mult dispozitivele IoT în operațiunile lor, aceste dispozitive pot deveni ținte potențiale pentru atacuri cibernetice. Dispozitivele IoT nesigure pot fi exploatate pentru a obține acces neautorizat la rețele sau pentru a lansa atacuri.
6. **Criptojacking.** Cryptojacking-ul implică utilizarea neautorizată a resurselor unui computer sau ale unei rețele pentru a mina criptomonede. Infractorii cibernetici pot infecta sistemele cu programe malware care minează în tăcere criptomonede, afectând performanța sistemului.
7. **Scriptare între site-uri (XSS).** Atacurile XSS implică injectarea de scripturi rău intenționate în paginile web vizualizate de alți utilizatori. Acest lucru poate duce la furtul datelor utilizatorilor, la deturnarea sesiunilor sau la răspândirea de programe malware către alți utilizatori.
8. **Injecție SQL.** Atacurile de injectare SQL apar atunci când codul SQL rău intenționat este injectat în câmpurile de introducere, permițând atacatorilor să manipuleze o bază de date. Acest lucru poate duce la acces neautorizat, manipularea datelor sau extragerea datelor.
9. **Malware fără fișiere.** Malware-ul fără fișiere funcționează în memorie, mai degrabă decât să se bazeze pe fișiere executabile. Acest lucru face mai dificilă detectarea soluțiilor antivirus tradiționale, deoarece este posibil să nu existe niciun fișier fizic de analizat.
10. **Credential Stuffing.** În atacurile de falsificare a acreditărilor, infractorii cibernetici folosesc combinații de nume de utilizator și parole furate de la un serviciu pentru a obține acces neautorizat la un alt serviciu în care utilizatorii au reutilizat acreditările.

11. **DNS Spoofing și Cache Poisoning.** DNS spoofing implică redirecționarea interogărilor sistemului de nume de domeniu (DNS) către site-uri rău intenționate. Cache poisoning manipulează datele cache DNS, conducând utilizatorii către destinații neintenționate și potențial dăunătoare.

După cum s-a menționat, raportul "ENISA Threat Landscape 2023" (Lella, 2023) arată că principalele amenințări la nivel mondial și în UE sunt: ransomware, malware, inginerie socială, amenințări împotriva datelor, refuzul serviciului, amenințări pe internet, manipularea informațiilor și atacuri asupra lanțului de aprovizionare.

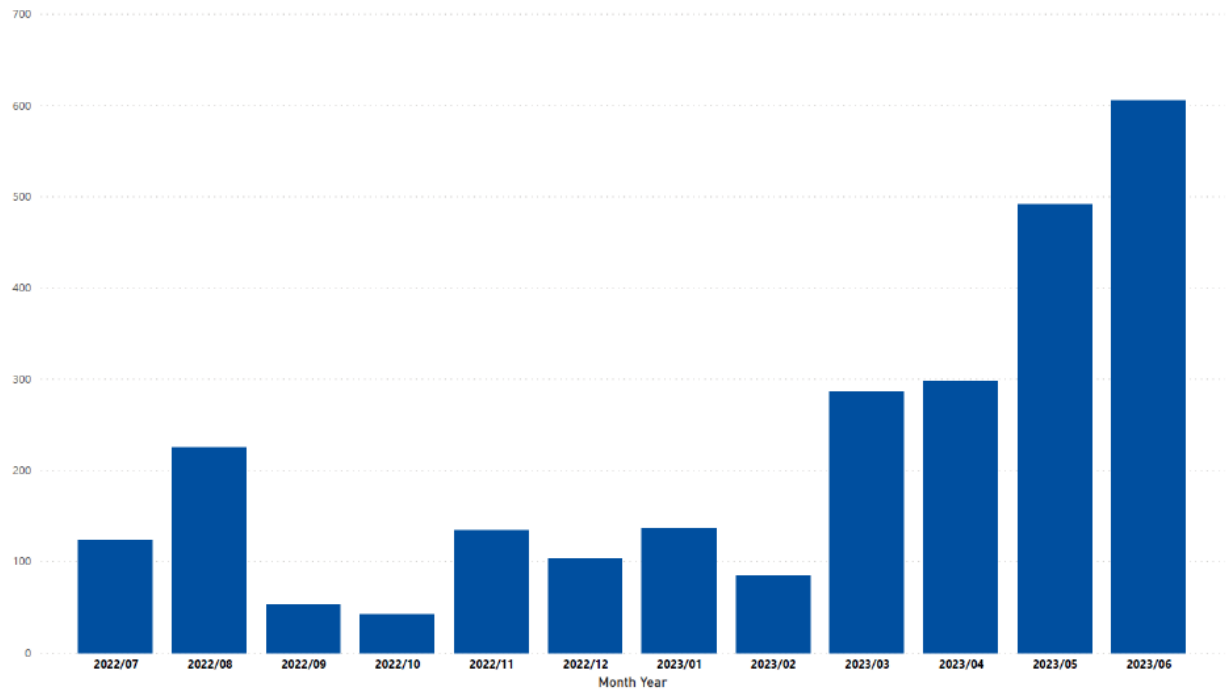


Figura 1. Cronologia evenimentelor din UE (numărul de incidente observate pe lună) (Lella, 2023)

Raportul ilustrează (figura 1) creșterea atacurilor cibernetice în prima parte a anului 2023. Această creștere se reflectă atât la nivel mondial, cât și la nivelul UE. Creșterea ar putea să nu reflecte doar creșterea numărului, ci și conștientizarea unor astfel de evenimente. Cu toate acestea, tendința este îngrijorătoare.

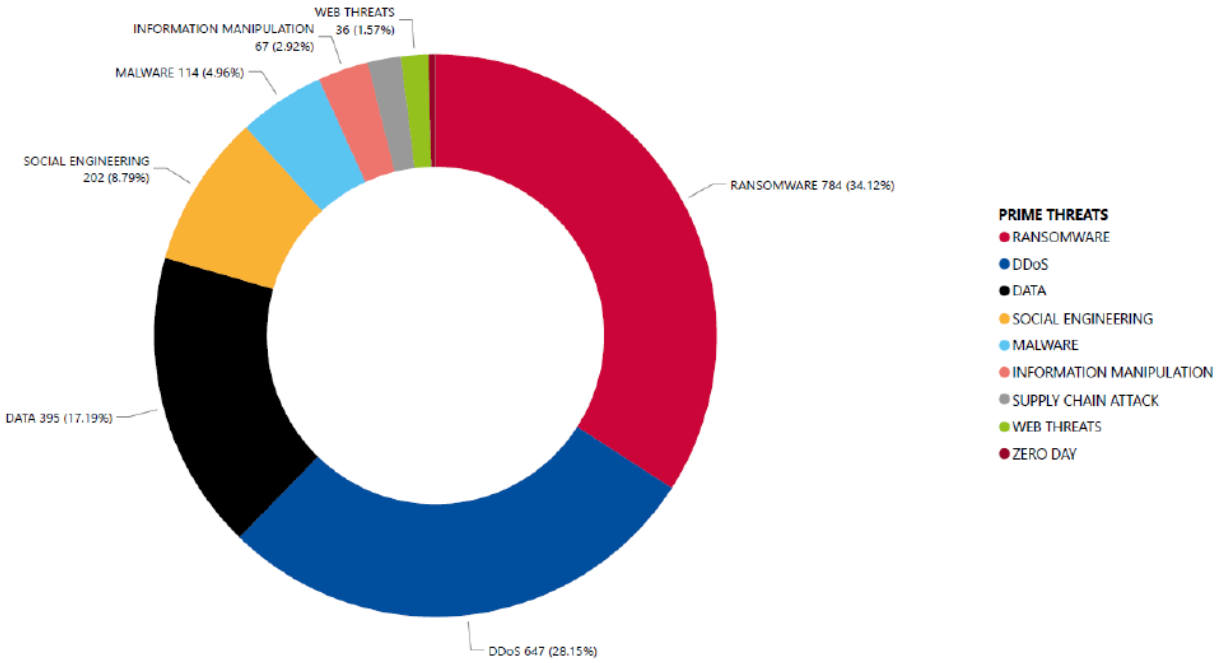


Figura 2. Defalcarea la nivelul UE a numărului de amenințări în funcție de grupul de amenințări (Lella, 2023)

Putem vedea în Figura 2 că cele mai frecvente amenințări au fost: Ransomware, Refuzul serviciului, Amenințări împotriva datelor, Inginerie socială și Malware. Acestea au fost urmate de manipularea informațiilor, atacurile lanțului de aprovizionare, amenințările pe internet și Zero Day.

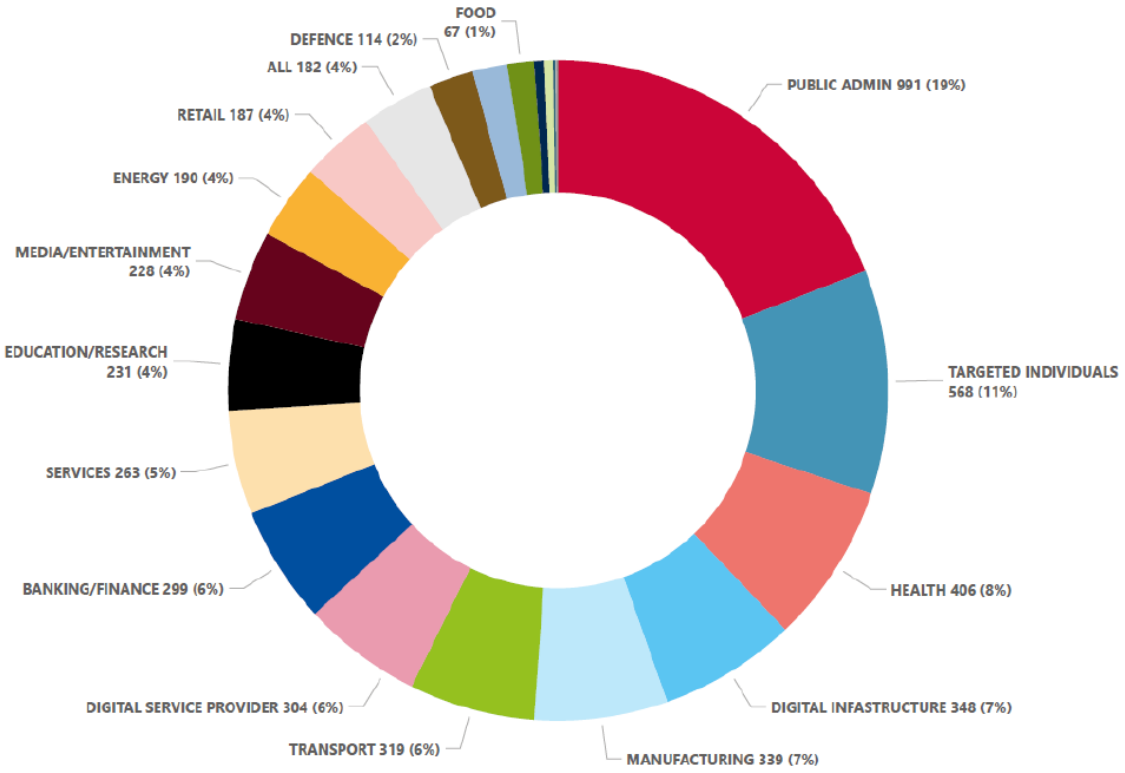


Figura 3. Sectoare vizate în funcție de numărul de incidente (iulie 2022 - iunie 2023) (Lella, 2023)

O analiză sectorială arată că amenințările depășesc granițele anumitor industrii sau sectoare, exercitându-și influența într-un spectru larg de domenii (Lella, 2023). Acest lucru s-ar putea datora interconectivității ridicate a lumii digitale de astăzi.

În peisajul global global, un număr mare de evenimente au vizat organizații din administrația publică (19%) și sănătate (8%). Putem observa că unul dintre principalii actori amenințați sunt persoanele fizice (11%). Chiar dacă acest lucru ar putea părea fără legătură cu startup-urile și sectorul privat, acești indivizi ar putea fi angajați într-un startup și ar putea pune neintenționat companiile în pericol.

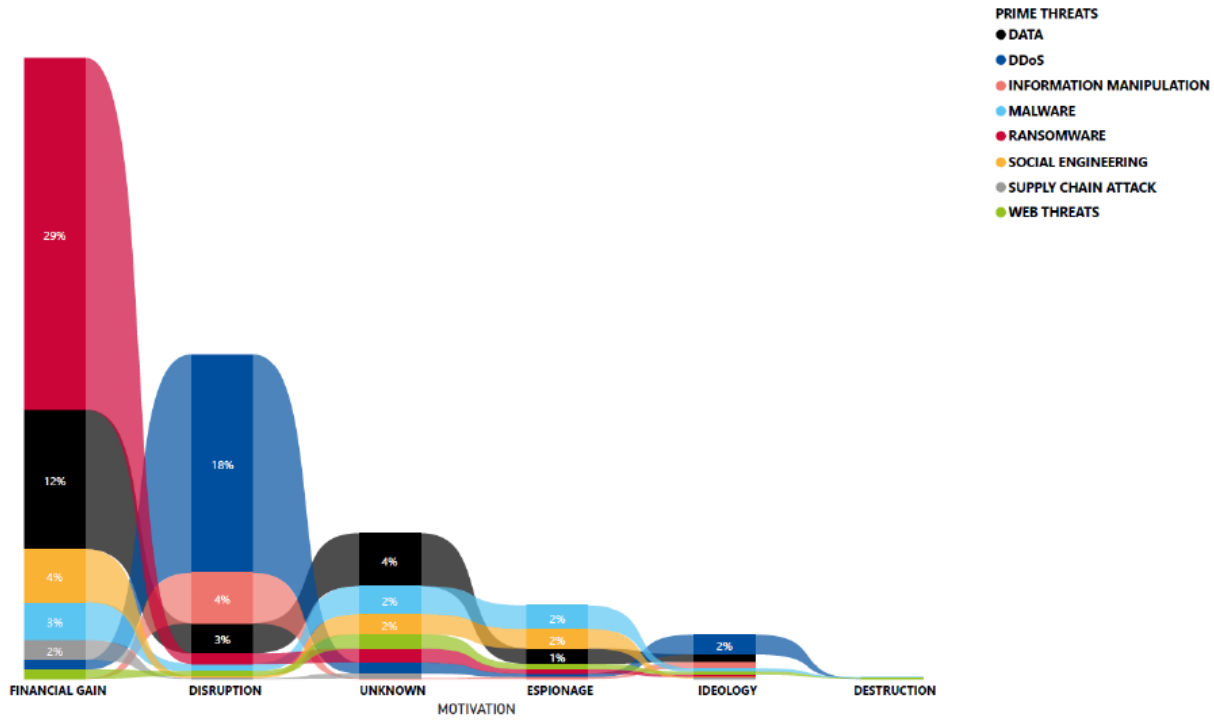


Figura 4. Motivația atacatorilor pe categorii de amenințări (Lella, 2023)

Raportul prezintă, de asemenea, motivațiile din spatele atacurilor cibernetice din perioada stabilită (Lella, 2023). După cum se poate observa din figura 4, majoritatea atacurilor au avut câștiguri financiare, urmate de perturbări, necunoscute, spionaj și ideologie. Ransomware-ul reprezintă aproape 30% din atacurile efectuate pentru câștiguri financiare, urmate de amenințări împotriva datelor, inginerie socială și malware.

Conștientizarea motivelor din spatele amenințărilor cibernetice și a tipurilor de amenințări ar putea furniza informațiile necesare și ghida strategia utilizată de startup-uri pentru a dezvolta și implementa practici de Igienă Digitală. De exemplu, startup-urile și sectorul privat sunt vizate în principal pentru câștiguri financiare. Știind că ransomware-ul, amenințările împotriva datelor, ingineria socială și malware-ul au fost utilizate în principal în astfel de scopuri, startup-urile și-ar putea concentra strategia de Igienă Digitală pe protejarea accesului la date și educarea clienților și angajaților pentru a se proteja de amenințările de inginerie socială.

Pentru a înțelege modul în care un startup ar trebui să abordeze amenințările cibernetice și ce trebuie să facă pentru a se proteja, am pregătit un exemplu de bună practică. Acest lucru va ilustra modul în care o companie ar trebui să facă față posibilelor amenințări și cum ar trebui să se pregătească pentru a preveni evenimentele cibernetice.

Unitatea 4 – 1 exemplu de bune practici pentru startup-uri

Pentru a înțelege mai bine cum să identificați amenințările și cum să gestionați situația în prealabil, să luăm în considerare următorul exemplu. Ne-am concentrat exemplul pe vulnerabilitatea care poate apărea din plata online, care este o situație răspândită și comună care poate afecta atât compania, cât și clienții aflați în situația unui atac cibernetic.

Igiena digitală în securitatea plăților online

Context

În contextul evoluției rapide al dezvoltării aplicațiilor mobile, unde inovația se intersectează cu tranzacțiile financiare, asigurarea securității unei aplicații care procesează plăți online devine primordială. Un exemplu este cel al unei companii care oferă un abonament la o aplicație mobilă, ceea ce ar putea ridica o vulnerabilitate asociată procesării plăților. Vulnerabilitatea potențială a sistemului lor de procesare a plăților online ar putea expune atât compania, cât și clienții săi la riscuri de fraudă financiară.

Startup-ul trebuie să analizeze situația, să identifice riscurile și să implementeze soluții pentru a preveni orice vulnerabilități și situații de fraudă financiară.

Pasul 1. Analiza situației

Ca prim pas în procesul de Igienă Digitală, avem analiza situației. În această fază, este important să identificați vulnerabilitățile și să evaluați riscul și implicațiile acestor vulnerabilități în cazul unei breșe de securitate.

Identificarea vulnerabilității securității plăților:

Compania a efectuat o analiză aprofundată a funcționalității aplicației de procesare a plăților pentru a identifica potențialele puncte slabe, inclusiv gateway-uri de plată nesigure, vulnerabilități în criptarea tranzacțiilor și potențiale puncte de acces neautorizat.

Efectuarea unei analize cuprinzătoare a unei aplicații de plată pentru a identifica potențialele puncte slabe implică o examinare sistematică și aprofundată a diferitelor componente din cadrul aplicației. O orientare generală pentru efectuarea unei astfel de analize ar putea include:

1. **Evaluarea riscurilor:** Identificați și înțelegeți componentele critice ale aplicației de plată, inclusiv autentificarea utilizatorilor, stocarea datelor, procesarea plăților și comunicarea cu serverele externe.

2. **Verificarea conformității cu reglementările:** Asigurați-vă că aplicația de plată respectă standardele de reglementare relevante și cerințele de conformitate din industrie, cum ar fi Standardul de securitate a datelor din industria cardurilor de plată (PCI DSS).
3. **Cartografierea fluxului de date:** Cartografiați fluxul de date sensibile (de exemplu, informații despre cardul de credit) în cadrul aplicației, de la intrare la stocare și transmitere. Identificați punctele potențiale de vulnerabilitate în acest flux de date.
4. **Securitatea rețelei:** Evaluați securitatea comunicațiilor în rețea, inclusiv utilizarea protocoalelor securizate (HTTPS), criptarea și certificatele SSL (secure sockets layer).
5. **Mecanisme de autentificare:** Evaluați capacitatea mecanismelor de autentificare a utilizatorilor. Implementați autentificarea multi-factor pentru a adăuga un nivel suplimentar de securitate.
6. **Securitatea gateway-ului de plată:** Examinați integrarea cu gateway-urile de plată, asigurându-vă că sunt utilizate servicii sigure și de renume. Actualizați și corectați periodic software-ul gateway-ului de plată.
7. **Criptarea datelor:** Implementați criptarea end-to-end pentru a proteja datele sensibile ale utilizatorilor pe parcursul întregului proces de tranzacție.
8. **Scanarea vulnerabilităților și testarea penetrării:** Efectuați scanări regulate ale vulnerabilităților și teste de penetrare pentru a identifica punctele slabe potențiale și pentru a simula scenarii de atac din lumea reală. Acest lucru poate implica utilizarea unor instrumente automate sau angajarea unor firme de securitate terțe cu experiență în testarea penetrării.
9. **Revizuirea codului:** Efectuați o examinare amănunțită a codului pentru a identifica orice vulnerabilități sau puncte slabe din codul sursă al aplicației. Asigurați-vă că practicile de codificare respectă cele mai bune practici de securitate.
10. **Plan de răspuns la incidente:** Dezvoltați și implementați un plan de răspuns la incidente pentru a aborda și a atenua prompt potențialele încălcări ale securității. Aceasta include existența unor proceduri pentru notificarea utilizatorilor în cazul unui incident de securitate.
11. **Audituri de securitate terță parte:** Luați în considerare angajarea firmelor de securitate terțe specializate în audituri de securitate a aplicațiilor. Aceste firme pot aduce o perspectivă independentă și expertiză specializată pentru a identifica vulnerabilitățile.

Puteți utiliza aceste puncte ca listă de verificare pentru a efectua analiza.

Securitatea este un proces continuu, iar revizuirile și actualizările periodice sunt esențiale pentru a rămâne cu un pas înaintea amenințărilor emergente. Punctele de pe lista de verificare menționată mai sus se pot schimba în timp, în funcție de posibilele amenințări și de domeniul securității cibernetice. Colaborarea cu firme de securitate sau consultanți terți poate oferi expertiză și informații suplimentare, în special atunci când vine vorba de audituri aprofundate de securitate și teste de penetrare. Este esențial să acordați

prioritate securității aplicațiilor de plată pentru a proteja atât afacerea, cât și utilizatorii acesteia de potențiale riscuri și încălcări.

Să presupunem că, în timpul unui audit de securitate de rutină, echipa de securitate a startup-ului identifică o potențială slăbiciune în protocolul de criptare utilizat pentru transmiterea datelor de plată în aplicația mobilă. Apoi, echipa trebuie să evalueze vulnerabilitatea și implicațiile acesteia pentru companie și utilizatori.

Evaluarea riscurilor și implicațiilor:

După identificarea vulnerabilităților de securitate a plăților, este important să se ia în considerare riscurile și implicațiile atât pentru companie, cât și pentru utilizatori. Această parte a procesului implică evaluarea riscurilor pentru companie și utilizatori și prioritizarea vulnerabilităților identificate în funcție de impactul potențial.

1. **Evaluarea impactului:** Evaluarea impactului potențial al unei încălcări a securității atât asupra companiei, cât și asupra utilizatorilor săi, luând în considerare pierderile financiare, daunele reputaționale și potențialele consecințe juridice.
2. **Prioritizare:** Prioritizați vulnerabilitățile pe baza gravității impactului potențial și a probabilității de exploatare.

În timpul evaluării riscurilor asociate cu slăbiciunea protocolului de criptare, echipa de securitate evaluează amploarea vulnerabilității, luând în considerare factori precum tipul de algoritm de criptare utilizat, domeniul de aplicare al exploatării potențiale și impactul asupra securității datelor utilizatorului.

Analiza de risc își propune să înțeleagă consecințele potențiale ale vulnerabilității de criptare, inclusiv riscul accesului neautorizat la informații sensibile de plată și impactul potențial asupra reputației companiei.

Pasul 2. Identificarea uneo soluții

Soluțiile pentru posibile vulnerabilități de securitate a plăților pot include:

1. **Integrare securizată a gateway-ului de plată:** Actualizați sistemul de procesare a plăților pentru a se integra cu un gateway de plată securizat, asigurându-vă că toate tranzacțiile sunt criptate și protejate de interceptare în timpul transmiterii.
2. **Criptare end-to-end:** Implementați criptarea end-to-end pentru toate tranzacțiile de plată, protejând datele sensibile ale utilizatorilor împotriva accesului neautorizat în fiecare etapă a procesului de tranzacție.

3. **Îmbunătățiri ale autentificării utilizatorilor:** Consolidați măsurile de autentificare a utilizatorilor, încorporând autentificarea multi-factor pentru a vă asigura că numai utilizatorii autorizați pot accesa și efectua tranzacții în cadrul aplicației.
4. **Audituri regulate de securitate și verificări de conformitate:** Instituiți audituri de securitate de rutină axate în mod special pe funcționalitatea de procesare a plăților, efectuând verificări de conformitate cu standardele și reglementările din industrie.

În cazul mai specific al deficienței din protocolul de criptare pe care l-am folosit ca exemplu, răspunsul și diminuarea ar include:

1. **Izolare imediată:** Compania ia măsuri imediate pentru a limita vulnerabilitatea prin dezactivarea temporară a protocolului de criptare afectat pentru a preveni orice exploatare potențială ulterioară.
2. **Comunicarea cu părțile interesate:** Compania inițiază o comunicare transparentă cu utilizatorii săi, notificându-i despre vulnerabilitatea de criptare identificată, suspendarea temporară a funcționalității afectate și eforturile continue de abordare a problemei.
3. **Implicarea experților în securitate:** Compania angajează serviciile experților externi în securitate cibernetică pentru a efectua o analiză aprofundată a vulnerabilității de criptare și pentru a oferi recomandări pentru o soluție de criptare mai robustă și mai sigură.
4. **Dezvoltarea unui patch:** Pe baza recomandărilor experților în securitate, echipa de dezvoltare creează un patch care abordează vulnerabilitatea criptării. Aceasta include implementarea unui algoritm de criptare mai sigur și asigurarea compatibilității cu sistemele existente.
5. **Testarea internă:** Înainte de implementarea patch-ului, compania efectuează teste interne amănunțite pentru a se asigura că măsurile de criptare actualizate nu introduc noi vulnerabilități sau perturbă funcționalitatea aplicației de plată.
6. **Implementarea patch-ului:** Odată ce patch-ul este considerat eficient și sigur, compania implementează actualizarea pe toate dispozitivele utilizatorilor, restabilind funcționalitatea de plată cu măsuri de criptare îmbunătățite.
7. **Monitorizarea post-implementare:** Compania monitorizează îndeaproape performanța aplicației post-implementare pentru a se asigura că patch-ul de criptare atenuează cu succes vulnerabilitatea și nu introduce probleme neprevăzute.
8. **Educarea utilizatorilor:** Pentru a reconstrui încrederea utilizatorilor, compania ar putea lansa o campanie educațională în cadrul aplicației, informând utilizatorii despre vulnerabilitatea de criptare și pașii făcuți pentru a o aborda și oferind sfaturi despre menținerea practicilor de utilizare sigure.

Pașii din acest răspuns sunt specifici problemei identificate. Dacă auditul de securitate identifică o problemă diferită, atunci vor fi implementate răspunsuri specifice pentru acea problemă.

Pasul 3. Resultate și impact

Abordarea companiei orientată către igiena digitală în securitatea aplicațiilor pentru plățile online a dat rezultate pozitive:

- Zero cazuri de tranzacții neautorizate sau încălcări ale securității pe parcursul unui an.
- Creșterea încrederii utilizatorilor în aplicație, ceea ce duce la o creștere a numărului de tranzacții și recenzii pozitive ale utilizatorilor.
- Respectarea reglementărilor din industrie, poziționarea companiei ca o platformă sigură și de încredere pentru plăți online.

Principalele idei de reținut

Startup-urile care oferă aplicații de procesare a plăților pot extrage informații valoroase din acest exemplu:

- Prioritizați integrarea gateway-urilor de plată securizate pentru a proteja datele tranzacțiilor.
- Implementați criptarea integrală pentru a proteja datele utilizatorilor pe tot parcursul procesului de plată.
- Îmbunătățiți măsurile de autentificare a utilizatorilor, încorporând autentificarea multi-factor pentru securitate suplimentară.
- Efectuați audituri regulate de securitate și verificări de conformitate pentru a fi cu un pas înaintea potențialelor vulnerabilități și pentru a asigura alinierea la standardele din domeniu.

Prin adoptarea acestor practici de igienă digitală, dezvoltatorii de aplicații de procesare a plăților pot contribui la crearea unei platforme sigure și fiabile, încurajând încrederea în rândul utilizatorilor implicați în tranzacții financiare online.

Referințe:

Mattioli, R.; Malatras, A.; Hunter, E.N.; Biasibetti Penso, M.G.; Bertram, D.; Neubert, I. (2023). Identifying Emerging Cyber Security Threats and Challenges for 2030. ENISA

Lella, I.; Tsekmezoglou, E.; Theocharidou, M.; Magonara, E.; Malatras, A.; Naydenov, R.S.; Ciobanu, C. (2023). ENISA Threat Landscape 2023. ENISA

Digital hygiene: the most important unfinished business: https://www.telefonica.com/en/communication-room/blog/digital-hygiene-the-most-important-unfinished-business/

What is Cyber Hygiene? Definition, Benefits, & Best Practices: https://securityscorecard.com/blog/what-is-cyber-hygiene-definition-benefits-best-practices/

What is cyber hygiene and why is it important?:

https://www.techtarget.com/searchsecurity/definition/cyber-hygiene