Handboek voor startups

BDA

mathemagenesis

MUĞLA SITKI KOÇMAN ÜNİVERSİTESİ

eLearning software

EduVibes

WITTENBORG University of Applied Sciences

29 VAN FEBRUARI 2024

Co-funded by the European Union

GOOD START

Good Digital Hygiene for Startups

Projectnr.: 2022-1-LV01-KA220-VET-000086725 | Titel van het project: Goede digitale hygiëne voor startups

Inhoudsopgave

Module 1 - Definities en concepten van digitale hygiëne begrijpen

Unit 1 - Conceptueel kader van digitale hygiëne

In het snel evoluerende landschap van digitaal ondernemerschap worden startups geconfronteerd met een groot aantal uitdagingen, variërend van hevige concurrentie tot beperkte middelen. Te midden van deze uitdagingen is het waarborgen van robuuste digitale hygiënepraktijken cruciaal voor de duurzame groei en het succes van de startups.

Het concept van digitale hygiëne is gebaseerd op verschillende theoretische kaders en principes uit verschillende vakgebieden, waaronder cyberbeveiliging, informatiebeheer en organisatiegedrag. Er zijn enkele belangrijke theorieën waarop het concept van digitale hygiëne is gebaseerd:

1. Theorie over cyberbeveiliging

De cybersecuritytheorie omvat verschillende principes en modellen die gericht zijn op het begrijpen en aanpakken van cyberdreigingen en kwetsbaarheden. De CIA-triade (Vertrouwelijkheid, Integriteit, Beschikbaarheid) is een fundamenteel concept in de cyberbeveiligingstheorie, waarbij het belang wordt benadrukt van het beschermen van gegevens tegen ongeoorloofde toegang (vertrouwelijkheid), het waarborgen van de nauwkeurigheid en betrouwbaarheid van gegevens (integriteit) en het handhaven van de toegankelijkheid van gegevens voor geautoriseerde gebruikers (beschikbaarheid). Andere cyberbeveiligingstheorieën, zoals het Defense-in-depth-model en het Zero Trust-model, bieden kaders voor het ontwerpen en implementeren van robuuste cyberbeveiligingsstrategieën om risico's te beperken en zich te verdedigen tegen cyberaanvallen.

2. Theorie van informatiemanagement

De informatiemanagementtheorie richt zich op het effectieve beheer van informatiemiddelen binnen organisaties. Het model voor het beheer van de levenscyclus van informatie is een theoretisch kader dat de stadia beschrijft waarin informatie wordt doorlopen van creatie tot verwijdering, waarbij het belang wordt benadrukt van het beheren van informatie gedurende de hele levenscyclus om vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen. De principes van gegevensbeheer, gegevensbeheer en gegevenskwaliteitsbeheer staan ook centraal in de theorie van informatiebeheer en geven aan hoe organisaties hun gegevensactiva effectief kunnen beheren en beschermen.

3. Theorie van menselijke factoren

De theorie van menselijke factoren onderzoekt de rol van menselijk gedrag, cognitie en besluitvorming in de context van cyberbeveiliging. De Human Error Theory suggereert dat menselijke fouten aanzienlijk bijdragen aan cyberbeveiligingsincidenten en datalekken, wat het belang benadrukt van training, bewustzijn en bruikbaarheid bij het beperken van mensgerelateerde risico's. De Theory of Planned Behavior en het Technology Acceptance Model (TAM) zijn andere theoretische kaders die uitleggen hoe de houding, overtuigingen en percepties van individuen hun gedrag beïnvloeden bij het toepassen van cyberbeveiligingspraktijken en -technologieën.

4. Theorie van organisatiegedrag

De theorie van organisatiegedrag onderzoekt hoe individuen, groepen en structuren binnen organisaties op elkaar inwerken en gedrag beïnvloeden. Het raamwerk technologie-organisatie-omgeving is een theoretisch model dat de factoren verklaart die van invloed zijn op de acceptatie en implementatie van informatietechnologieën binnen organisaties, waaronder technologische factoren, organisatorische factoren en omgevingsfactoren. De theorie van de diffusie van innovaties, ontwikkeld door Everett Rogers, onderzoekt hoe nieuwe ideeën, technologieën en praktijken zich verspreiden binnen samenlevingen en organisaties, en biedt inzicht in de acceptatie en verspreiding van digitale hygiënepraktijken binnen startups en andere organisatorische contexten.

5. Theorie van naleving

De nalevingstheorie richt zich op de factoren die van invloed zijn op de naleving van regels, voorschriften en normen door individuen en organisaties. De theorie van gepland gedrag en de theorie van beredeneerd handelen zijn theoretische modellen die de intentie van individuen om te voldoen aan regels en voorschriften verklaren op basis van hun houding, subjectieve normen en waargenomen gedragscontrole. Deze theorieën geven inzicht in hoe startups en organisaties de naleving van cyberbeveiligingsvoorschriften en -normen kunnen bevorderen door middel van onderwijs, training, stimulansen en handhavingsmechanismen.

Het concept van digitale hygiëne integreert dus multidisciplinaire perspectieven en benaderingen om de complexe uitdagingen van cyberbeveiliging, informatiebeheer, menselijk gedrag en organisatorische dynamiek binnen startups en andere organisaties aan te pakken.

Aanvullende concepten bieden ook een basis voor het begrijpen en implementeren van digitale hygiënepraktijken binnen startups, waardoor de bescherming, integriteit en veerkracht van hun digitale infrastructuur en activiteiten worden gewaarborgd:

a) Cyberbeveiliging

Cyberbeveiliging is de praktijk van het beschermen van digitale systemen, netwerken en gegevens tegen ongeoorloofde toegang, cyberaanvallen en datalekken. Het omvat verschillende technologieën, processen en praktijken die gericht zijn op het beschermen van digitale activa en het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

B) Gegevensbescherming

Gegevensprivacy verwijst naar de bescherming van persoonlijke en gevoelige informatie tegen ongeoorloofde toegang, gebruik of openbaarmaking. Het gaat om naleving van voorschriften en normen voor het verzamelen, opslaan en verwerken van gegevens, zoals GDPR, HIPAA of CCPA, om de privacyrechten van individuen te beschermen.

C) Risicobeheer

Risicobeheer omvat het identificeren, beoordelen en beperken van risico's die gepaard gaan met het opereren in een digitale omgeving. Het omvat het implementeren van controles en maatregelen om potentiële bedreigingen en kwetsbaarheden te voorkomen, op te sporen en erop te reageren die van invloed kunnen zijn op de activiteiten, reputatie of financiële stabiliteit van een startup.

D) Nalevings- en regelgevingskaders

Naleving van regelgeving en industrienormen is essentieel voor startups om legale en ethische operaties te garanderen. Regelgevingskaders, zoals GDPR, HIPAA, PCI DSS of SOX, bieden richtlijnen en vereisten voor gegevensbescherming, beveiliging en privacy waaraan startups zich moeten houden om juridische en financiële gevolgen te voorkomen.

E) Managementsystemen voor informatiebeveiliging (ISMS)

ISMS-frameworks, zoals ISO/IEC 27001, bieden een systematische aanpak voor het beheren en beschermen van informatiemiddelen binnen organisaties. Ze omvatten beleid, procedures en controles voor het beheren van risico's, het waarborgen van naleving en het voortdurend verbeteren van informatiebeveiligingspraktijken.

F) Gegevensbeheer

Gegevensbeheer verwijst naar het beheer van en toezicht op gegevensactiva binnen een organisatie. Het omvat het vaststellen van beleid, processen en controles voor gegevenskwaliteit, -integriteit en -beveiliging om ervoor te zorgen dat gegevens effectief, verantwoord en ethisch worden beheerd.

G) Reactie op incidenten en planning van bedrijfscontinuïteit

Incidentrespons en bedrijfscontinuïteitsplanning omvatten het voorbereiden op en reageren op cyberbeveiligingsincidenten en verstoringen. Startups moeten uitgebreide incidentresponsplannen en

bedrijfscontinuïteitsstrategieën ontwikkelen om de impact van cyberaanvallen, datalekken of andere verstoringen op hun activiteiten en reputatie te beperken.

Digitale hygiëne omvat dus het geheel van praktijken en protocollen die gericht zijn op het handhaven van de veiligheid, efficiëntie en integriteit van digitale activa en operaties. Dit conceptuele kader schetst de belangrijkste componenten van digitale hygiëne die zijn afgestemd op de unieke behoeften en beperkingen van startups.

Het schema van het conceptuele kader van digitale hygiëne voor startups is weergegeven in figuur 1.

Figuur 1. Schema van conceptueel kader van digitale hygiëne voor startups

Dit schema schetst de vier belangrijkste componenten van digitale hygiëne voor startups: digitale infrastructuur, gegevensbeheer, cyberbeveiliging en operationele veerkracht. Elk onderdeel omvat specifieke

praktijken en protocollen die gericht zijn op het waarborgen van de veiligheid, efficiëntie en integriteit van digitale activa en operaties binnen een startup-omgeving.

Digitale infrastructuur omvat de hardware, software en cloudservices die door startups worden gebruikt om hun activiteiten te ondersteunen en producten of diensten te leveren. Het omvat apparaten zoals computers, servers en netwerkapparatuur, evenals softwaretoepassingen en platforms.

Gegevensbeheer omvat het beheer, de opslag en de bescherming van gegevensactiva binnen een startup. Het omvat het verzamelen, opslaan, gebruiken en delen van gegevens, evenals naleving van wettelijke vereisten en bescherming tegen datalekken.

Cyberbeveiliging richt zich op het beschermen van digitale activa en activiteiten tegen cyberdreigingen zoals malware, phishing-aanvallen en ongeoorloofde toegangspogingen. Het gaat om het inzetten van proactieve maatregelen om beveiligingsincidenten effectief te detecteren, te voorkomen en erop te reageren.

Operationele veerkracht omvat het waarborgen van de continuïteit en veerkracht van de bedrijfsvoering in het licht van ontwrichtende gebeurtenissen zoals natuurrampen, cyberaanvallen of systeemstoringen. Het omvat plannings-, paraatheids- en responsmaatregelen om downtime te minimaliseren en kritieke bedrijfsfuncties te behouden.

Figuur 2 toont het digitale hygiëneproces en de factoren ervan bij opstartactiviteiten.

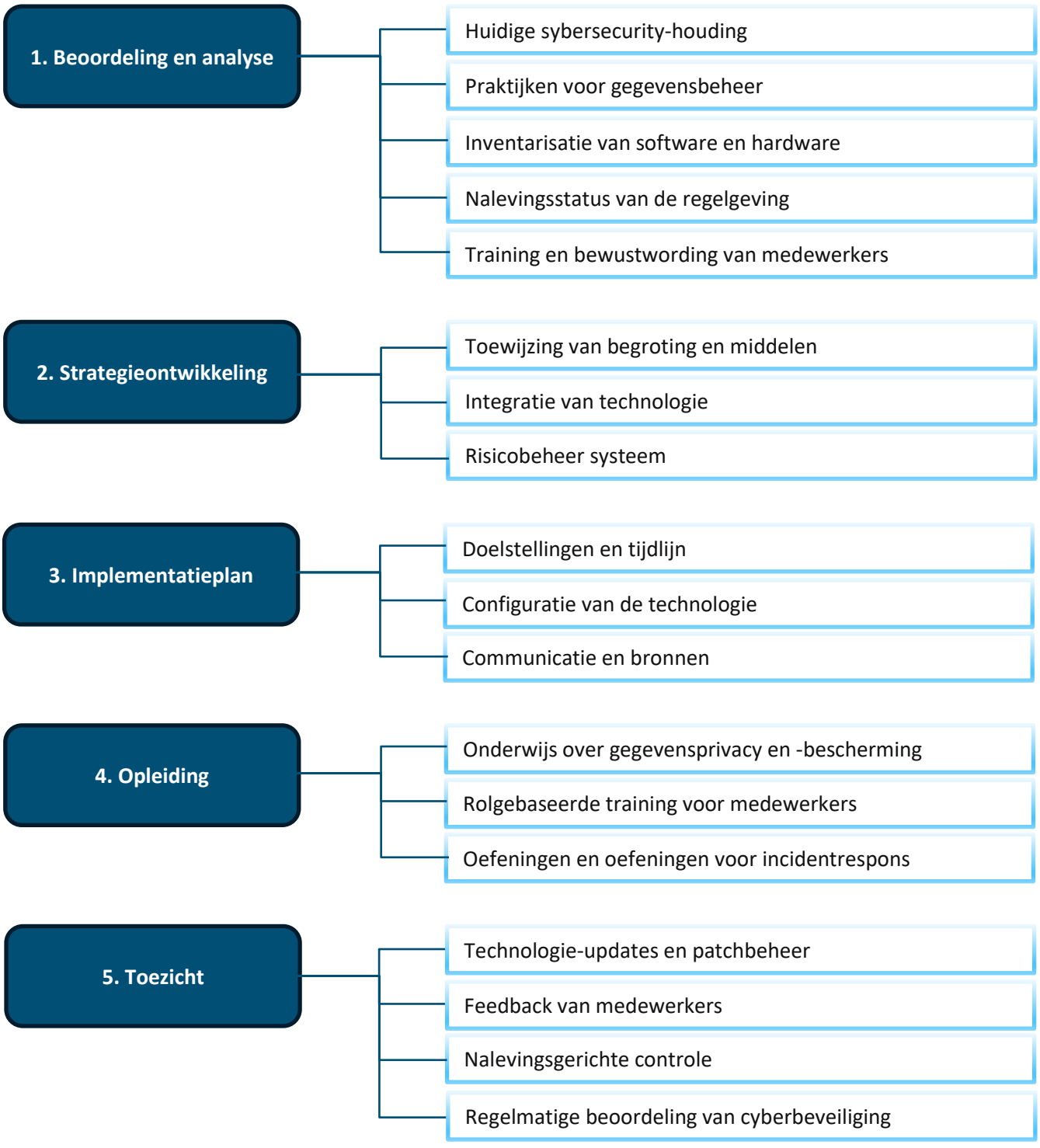
Deze gedetailleerde figuur illustreert het uitgebreide digitale hygiëneproces in een startup, waarbij de belangrijkste factoren en componenten in elke fase worden benadrukt, van beoordeling en analyse tot continue monitoring en verbetering.

De startup voert een grondige beoordeling uit van zijn huidige digitale praktijken en kwetsbaarheden en analyseert potentiële risico's en bedreigingen voor zijn digitale infrastructuur en gegevens. Op basis van de bevindingen van de beoordeling ontwikkelt de startup een uitgebreide digitale hygiënestrategie die is afgestemd op zijn behoeften en doelen, waarbij prioriteit wordt gegeven aan verbeterpunten.

De startup definieert duidelijke doelstellingen en tijdlijnen voor het implementeren van digitale hygiënemaatregelen en het effectief toewijzen van middelen, waaronder budget, personeel en technologie. De startup biedt trainingssessies en educatief materiaal voor werknemers over best practices op het gebied van digitale beveiliging, waardoor een cultuur van bewustzijn en verantwoordelijkheid op het gebied van cyberbeveiliging binnen de organisatie wordt bevorderd.

De startup monitort en evalueert voortdurend zijn inspanningen op het gebied van digitale hygiëne en voert regelmatig audits en beoordelingen uit om verbeterpunten te identificeren en aan te passen aan veranderende bedreigingen en uitdagingen.

Kortom, effectieve digitale hygiënepraktijken zijn onmisbaar voor startups die hun weg willen vinden in het complexe en dynamische landschap van digitaal ondernemerschap. Door het hierin beschreven conceptuele kader te implementeren, kunnen startups hun digitale infrastructuur versterken, hun gegevensactiva beschermen en hun cyberbeveiliging verbeteren.



Figuur 2. Digitaal hygiëneproces en de factoren ervan bij het opstarten

Unit 2 - De noodzakelijkheden/essentials van goede digitale hygiëne voor startups

In het digitale tijdperk van vandaag zijn startups sterk afhankelijk van technologie om innovatie te stimuleren, activiteiten te stroomlijnen en klanten te bereiken. De voordelen van technologie brengen echter risico's met zich mee, waaronder cyberdreigingen, datalekken en operationele verstoringen. Om deze uitdagingen het hoofd te bieden en succes op de lange termijn te garanderen, moeten startups prioriteit geven aan goede digitale hygiënepraktijken.

Goede digitale hygiënepraktijken omvatten een reeks proactieve maatregelen en protocollen die gericht zijn op het beschermen van de digitale activa, infrastructuur en gegevens van een startup tegen mogelijke bedreigingen, kwetsbaarheden en risico's.

De vereisten van een goede digitale hygiëne voor het opstarten:

1. Bescherming tegen cyberdreigingen en -aanvallen

Een van de belangrijkste redenen voor het handhaven van goede digitale hygiënepraktijken is om startups te beschermen tegen cyberdreigingen en -aanvallen. In een tijdperk waarin cybercriminaliteit toeneemt, zijn startups belangrijke doelwitten voor kwaadwillenden die misbruik willen maken van kwetsbaarheden in hun digitale infrastructuur en systemen. Cyberaanvallen, zoals malware-infecties, phishing-zwendel, ransomware-aanvallen en datalekken, kunnen verwoestende gevolgen hebben voor startups, waaronder financiële verliezen, reputatieschade, juridische aansprakelijkheid en operationele verstoringen. Door robuuste cyberbeveiligingsmaatregelen te implementeren, kunnen startups hun verdediging versterken en de risico's van cyberdreigingen beperken, hun kritieke activa beschermen en de bedrijfscontinuïteit waarborgen.

2. Bescherming van gevoelige gegevens en intellectueel eigendom

Startups hebben vaak te maken met gevoelige gegevens, waaronder klantinformatie, eigen technologieën, handelsgeheimen en intellectueel eigendom. Het handhaven van goede digitale hygiënepraktijken is essentieel om deze gevoelige informatie te beschermen tegen ongeoorloofde toegang, diefstal of compromittering. Datalekken en ongeoorloofde openbaarmaking kunnen niet alleen leiden tot financiële verliezen en juridische aansprakelijkheden, maar ook het vertrouwen van de klant ondermijnen, waardoor de reputatie en het merkimago van de startup worden aangetast. Door gegevensversleuteling, toegangscontroles en maatregelen ter voorkoming van gegevensverlies te implementeren, kunnen startups

hun gevoelige gegevensactiva beschermen en de vertrouwelijkheid, integriteit en beschikbaarheid van informatie behouden, waardoor het vertrouwen van klanten, partners en belanghebbenden behouden blijft.

3. Verbetering van de operationele efficiëntie en productiviteit

Goede digitale hygiënepraktijken dragen ook bij aan het verbeteren van de operationele efficiëntie en productiviteit binnen startups. Verouderde software, niet-gepatchte systemen en inefficiënte digitale workflows kunnen de productiviteit belemmeren, de samenwerking belemmeren en de groei van het bedrijf belemmeren. Door hun digitale infrastructuur regelmatig te onderhouden en bij te werken, kunnen startups de prestaties optimaliseren, processen stroomlijnen en knelpunten wegnemen, waardoor werknemers efficiënter en effectiever kunnen werken. Bovendien kunnen startups, door gebruik te maken van automatisering, cloudtechnologieën en digitale tools, workflows stroomlijnen, routinetaken automatiseren en de besluitvorming verbeteren, innovatie en concurrentievermogen op de markt stimuleren.

4. Zorgen voor naleving van de regelgeving en wettelijke verplichtingen

Naleving van wettelijke vereisten en wettelijke verplichtingen is een ander cruciaal aspect van het handhaven van goede digitale hygiënepraktijken. Startups die in verschillende sectoren actief zijn, zijn onderworpen aan een groot aantal wetten, voorschriften en nalevingsnormen met betrekking tot gegevensprivacy, -beveiliging en -bescherming. Het niet naleven van deze voorschriften kan leiden tot zware straffen, boetes en juridische gevolgen, waardoor de levensvatbaarheid en reputatie van de startup in gevaar komen. Door zich te houden aan wettelijke vereisten, zoals GDPR, HIPAA, PCI DSS of SOX, kunnen startups aantonen dat ze zich inzetten voor ethische bedrijfspraktijken, het vertrouwen van klanten en belanghebbenden winnen en juridische en financiële risico's beperken.

5. Bevordering van innovatie

Ten slotte is het handhaven van goede digitale hygiënepraktijken essentieel voor het bevorderen van innovatie en aanpassingsvermogen binnen startups. In de digitale economie van vandaag, waar technologische vooruitgang en marktverstoringen aan de orde van de dag zijn, moeten startups wendbaar, veerkrachtig en aanpasbaar blijven om te gedijen in een concurrerend landschap. Door opkomende technologieën te omarmen, digitale transformatie te omarmen en een cultuur van continue verbetering en leren te cultiveren, kunnen startups zich positioneren voor succes en duurzaamheid op de lange termijn, innovatie stimuleren en waarde creëren voor hun klanten en belanghebbenden.

Kortom, het handhaven van goede digitale hygiënepraktijken is onmisbaar voor startups die op zoek zijn naar succes, groei en veerkracht op de lange termijn.

.

Unit 3 - Het belang van digitale hygiëne

Het belang van een goede digitale hygiëne kan niet genoeg worden benadrukt. Van het beschermen van gevoelige gegevens tot het beperken van cyberdreigingen, digitale hygiënepraktijken zijn essentieel voor zowel individuen als organisaties. In deze casestudy onderzoeken we het belang van digitale hygiëne door de lens van een praktijkvoorbeeld, waarbij we de impact ervan op beveiliging, productiviteit en algemeen welzijn benadrukken.

Om het belang van digitale hygiëne te begrijpen, kunt u enkele digitale hygiënepraktijken bekijken.

1. Maak kennis met TechGenius, een dynamische startup gevestigd in Silicon Valley, gespecialiseerd in het ontwikkelen van geavanceerde softwareoplossingen voor bedrijven. TechGenius, opgericht in 2015, kreeg snel bekendheid in de technische industrie, trok toptalent aan en haalde spraakmakende klanten binnen. Naarmate het bedrijf zijn activiteiten en personeelsbestand uitbreidde, kwam het echter voor nieuwe uitdagingen te staan bij het beheer van zijn digitale infrastructuur en het beschermen van zijn digitale activa.

TechGenius opereerde, net als veel startups, in een snelle omgeving waar innovatie en efficiëntie voorop stonden. Te midden van de drukte van de dagelijkse bedrijfsvoering verzuimde het bedrijf echter prioriteit te geven aan digitale hygiënepraktijken. Werknemers gebruikten vaak zwakke wachtwoorden, werkten software niet regelmatig bij en negeerden basisbeveiligingsprotocollen, waardoor het bedrijf kwetsbaar was voor cyberdreigingen zoals phishing-aanvallen en datalekken.

TechGenius realiseerde zich het cruciale belang van digitale hygiëne en begon aan een reis om zijn benadering van cyberbeveiliging en gegevensbeheer te vernieuwen. Het bedrijf lanceerde een uitgebreid initiatief voor digitale hygiëne gericht op het opleiden van werknemers, het implementeren van best practices en het versterken van de beveiligingshouding.

Het digitale hygiëne-initiatief van TechGenius bestond uit verschillende belangrijke onderdelen:

1. Training en bewustwording van medewerkers. Het bedrijf organiseerde uitgebreide trainingssessies om werknemers voor te lichten over het belang van digitale hygiëne. Onderwerpen die aan bod kwamen, waren onder meer wachtwoordbeheer, e-mailbeveiliging, veilig browsen en regelgeving inzake gegevensbescherming. Door middel van interactieve workshops en online modules kregen medewerkers een beter inzicht in cyberbeveiligingsrisico's en hun rol bij het beperken ervan.

2. Beleidsontwikkeling en -handhaving. TechGenius heeft robuuste digitale hygiënebeleidslijnen en -procedures ontwikkeld om het gedrag van werknemers te beheersen en ervoor te zorgen dat de industrienormen worden nageleefd. Dit beleid had betrekking op gebieden zoals de complexiteit van wachtwoorden, software-updates, toegangscontroles en protocollen voor incidentrespons. Om de

verantwoordingsplicht te versterken, heeft het bedrijf regelmatige audits en handhavingsmechanismen geïmplementeerd om de naleving van dit beleid te controleren.

3. Technologische oplossingen. Naast onderwijs en beleidsmaatregelen investeerde TechGenius in technologische oplossingen om zijn digitale hygiënepraktijken te verbeteren. Dit omvatte de implementatie van multi-factor authenticatie, encryptietechnologieën, endpoint-beveiligingssoftware en netwerkbewakingstools. Door gebruik te maken van deze technologieën versterkte het bedrijf zijn verdediging tegen cyberdreigingen en beschermde het zijn digitale infrastructuur.

De implementatie van het digitale hygiëne-initiatief van TechGenius heeft belangrijke resultaten opgeleverd:

A. Verbeterde beveiligingshouding. Door prioriteit te geven aan digitale hygiëne heeft TechGenius zijn beveiligingspositie versterkt en het risico op cyberdreigingen verminderd. Incidenten zoals phishing-aanvallen en datalekken kwamen minder vaak voor, waardoor de potentiële impact op de activiteiten en reputatie van het bedrijf tot een minimum werd beperkt.

B. Verbeterde productiviteit. Met minder beveiligingsincidenten konden werknemers zich meer concentreren op hun kernverantwoordelijkheden, wat leidde tot een hogere productiviteit en efficiëntie in de hele organisatie. Door digitale workflows te stroomlijnen en downtime te minimaliseren, behaalde TechGenius betere resultaten en leverde het superieure resultaten aan zijn klanten.

C. Beschermde reputatie. Als vertrouwde leverancier van softwareoplossingen hangt de reputatie van TechGenius af van zijn vermogen om klantgegevens te beschermen en hoge beveiligingsnormen te handhaven. Door zich in te zetten voor digitale hygiëne, won het bedrijf het vertrouwen van zijn klanten en positioneerde het zich als een betrouwbare partner in een steeds competitievere markt.

D. Kostenbesparingen. Hoewel investeren in digitale hygiëne initiële kosten met zich mee kan brengen, wegen de voordelen op de lange termijn ruimschoots op tegen de kosten. TechGenius ervoer kostenbesparingen in termen van minder cybersecurity-incidenten, lagere nalevingsboetes en verhoogde operationele efficiëntie. Door kwetsbaarheden in de beveiliging proactief aan te pakken, vermeed het bedrijf potentieel kostbare gevolgen in verband met datalekken en niet-naleving van de regelgeving.

De case van TechGenius onderstreept het cruciale belang van digitale hygiëne in het digitale landschap van vandaag. Door prioriteit te geven aan onderwijs, beleidsontwikkeling en technologische oplossingen op het gebied van cyberbeveiliging, was TechGenius in staat om cyberdreigingen te beperken, de productiviteit te verhogen en zijn reputatie en bedrijfsresultaten te beschermen. Dit praktijkvoorbeeld dient als bewijs van de transformerende kracht van digitale hygiëne bij het beveiligen van organisaties tegen evoluerende cyberrisico's en het stimuleren van duurzame groei en succes.

Een ander voorbeeld van het belang van digitale hygiënepraktijken is het geval van SecureHealth.

SecureHealth is een startup voor zorgtechnologie die een revolutie teweegbrengt in de manier waarop medische dossiers worden beheerd en geraadpleegd. Met een cloudgebaseerd platform dat is ontworpen om de patiëntenzorg te stroomlijnen en de zorgresultaten te verbeteren, heeft SecureHealth snel aan populariteit gewonnen in de gezondheidszorg. Te midden van de snelle groei en acceptatie van zijn platform staat het bedrijf echter voor aanzienlijke uitdagingen bij het waarborgen van de veiligheid en privacy van patiëntgegevens.

Zorgorganisaties zijn belangrijke doelwitten voor cyberaanvallen vanwege de gevoelige aard van de gegevens die ze verwerken. SecureHealth erkent het cruciale belang van digitale hygiëne bij het waarborgen van de vertrouwelijkheid van patiënten en het handhaven van de naleving van de regelgeving. Met de complexiteit van IT-systemen voor de gezondheidszorg en het steeds evoluerende bedreigingslandschap moet het bedrijf echter waakzaam en proactief blijven bij het aanpakken van cyberbeveiligingsrisico's.

SecureHealth hanteert een proactieve benadering van digitale hygiëne en implementeert een uitgebreid cyberbeveiligingsprogramma dat is afgestemd op de unieke behoeften van de gezondheidszorg. Het bedrijf geeft prioriteit aan de volgende belangrijke componenten:

1. Gegevensversleuteling en toegangscontrole. SecureHealth versleutelt patiëntgegevens zowel in rust als tijdens het transport, zodat gevoelige informatie beschermd blijft tegen ongeoorloofde toegang. Toegangscontroles worden geïmplementeerd om de toegang tot patiëntendossiers te beperken tot alleen geautoriseerde beroepsbeoefenaren in de gezondheidszorg, waardoor het risico op datalekken tot een minimum wordt beperkt.

2. Regelmatige beveiligingsaudits en penetratietests. SecureHealth voert regelmatig beveiligingsaudits en penetratietests uit om kwetsbaarheden in haar systemen en infrastructuur te identificeren. Door proactief zwakke plekken in de beveiliging te identificeren en te verhelpen, versterkt het bedrijf zijn verdediging tegen cyberdreigingen en zorgt het voor naleving van gezondheidsvoorschriften zoals HIPAA.

3. Training en bewustwording van medewerkers. SecureHealth biedt uitgebreide cyberbeveiligingstraining aan alle medewerkers en benadrukt het belang van digitale hygiëne bij het beschermen van patiëntgegevens. Werknemers leren hoe ze beveiligingsbedreigingen kunnen herkennen en erop kunnen reageren, veilige praktijken kunnen implementeren in hun dagelijkse workflows en zich kunnen houden aan het bedrijfsbeleid en de procedures.

De implementatie van de digitale hygiëne-initiatieven van SecureHealth heeft tastbare resultaten opgeleverd:

A. Beschermde patiëntgegevens. Door prioriteit te geven aan digitale hygiëne, zorgt SecureHealth voor de vertrouwelijkheid, integriteit en beschikbaarheid van patiëntgegevens, waardoor het vertrouwen tussen zowel zorgverleners als patiënten wordt bevorderd.

B. Naleving van de regelgeving. SecureHealth handhaaft de naleving van zorgvoorschriften zoals HIPAA, waarmee het aantoont dat het zich inzet voor de bescherming van de privacy van patiënten en voldoet aan de industrienormen voor gegevensbeveiliging en vertrouwelijkheid.

C. Verminderd risico op datalekken. Met robuuste cyberbeveiligingsmaatregelen minimaliseert SecureHealth het risico op datalekken en andere beveiligingsincidenten, waardoor de reputatie wordt beschermd en de mogelijke financiële en juridische gevolgen tot een minimum worden beperkt.

De ervaring van SecureHealth benadrukt het cruciale belang van digitale hygiëne in de gezondheidszorg, waar er veel op het spel staat en de gevolgen van inbreuken op de beveiliging ernstig kunnen zijn. Door prioriteit te geven aan cyberbeveiligingsmaatregelen zoals gegevensversleuteling, toegangscontroles, regelmatige audits en training van werknemers, zorgt SecureHealth voor de veiligheid en integriteit van patiëntgegevens, wat uiteindelijk bijdraagt aan verbeterde patiëntenzorg en resultaten.

Om het belang van digitale hygiëne te begrijpen, kunt u overwegen aanvullende digitale hygiënepraktijken te onderzoeken.

FinTech Innovations is een startup die de financiële dienstverlening ontwricht met innovatieve digitale bankoplossingen. Door gebruik te maken van geavanceerde technologie zoals blockchain en kunstmatige intelligentie, biedt FinTech Innovations veilige, gebruiksvriendelijke bankdiensten aan zowel consumenten als bedrijven. Naarmate het bedrijf echter groeit en zijn klantenbestand uitbreidt, wordt het geconfronteerd met toenemende cyberbeveiligingsrisico's die de veiligheid en stabiliteit van zijn platform bedreigen.

Financiële instellingen zijn belangrijke doelwitten voor cyberaanvallen vanwege de waardevolle financiële gegevens die ze bezitten. FinTech Innovations erkent het belang van digitale hygiëne om het vertrouwen van haar klanten en partners te behouden. Met de complexiteit van financiële transacties en de evoluerende aard van cyberdreigingen, moet het bedrijf echter waakzaam en proactief blijven bij het beschermen van zijn digitale activa en infrastructuur.

FinTech Innovations implementeert een robuust digitaal hygiëneprogramma om cyberbeveiligingsrisico's aan te pakken en zijn platform te beschermen. Het bedrijf richt zich op de volgende belangrijke initiatieven:

1. Veilige authenticatie en autorisatie. FinTech Innovations implementeert sterke authenticatiemechanismen zoals biometrische authenticatie en multi-factor authenticatie om de identiteit van gebruikers te verifiëren en ongeoorloofde toegang tot accounts en transacties te voorkomen.

2. Real-time opsporing van fraude. FinTech Innovations maakt gebruik van geavanceerde analyse- en machine learning-algoritmen om frauduleuze activiteiten in realtime te detecteren en te voorkomen. Door transactiepatronen en gebruikersgedrag te analyseren, kan het bedrijf verdachte activiteiten identificeren en proactieve maatregelen nemen om frauderisico's te beperken.

3. Continue bewaking. FinTech Innovations houdt haar systemen en netwerken continu in de gaten om beveiligingsincidenten snel te detecteren en erop te reageren. Het bedrijf heeft een toegewijd team van cyberbeveiligingsprofessionals in dienst die verdachte activiteiten monitoren, beveiligingswaarschuwingen onderzoeken en tijdige herstelmaatregelen implementeren om potentiële bedreigingen aan te pakken.

De implementatie van de digitale hygiëne-initiatieven van FinTech Innovations heeft geleid tot belangrijke resultaten:

A. Groter vertrouwen van de klant. Door prioriteit te geven aan digitale hygiëne, toont FinTech Innovations zijn toewijding aan het beschermen van klantgegevens en financiële activa en het opbouwen van vertrouwen bij zijn gebruikers en belanghebbenden.

B. Minder fraude en minder beveiligingsincidenten. Met geavanceerde fraudedetectiemechanismen en continue monitoring minimaliseert FinTech Innovations het risico op fraude en beveiligingsincidenten, waardoor de veiligheid en integriteit van zijn platform en transacties worden gewaarborgd.

C. Bedrijfscontinuïteit en veerkracht. Door cyberbeveiligingsrisico's proactief aan te pakken, verbetert FinTech Innovations zijn weerbaarheid tegen cyberdreigingen en -verstoringen, waardoor de ononderbroken levering van financiële diensten aan zijn klanten en partners wordt gegarandeerd.

De ervaring van FinTech Innovations onderstreept het cruciale belang van digitale hygiëne in de financiële dienstverlening, waar veiligheid en vertrouwen van het grootste belang zijn. Door robuuste cyberbeveiligingsmaatregelen te implementeren, zoals veilige authenticatie, fraudedetectie en continue monitoring, zorgt FinTech Innovations voor de veiligheid en stabiliteit van zijn platform, wat uiteindelijk bijdraagt aan een veiligere en veiligere digitale bankervaring voor zijn klanten

Deze voorbeelden illustreren de cruciale rol van digitale hygiëne bij het beschermen van gevoelige gegevens, het handhaven van de naleving van de regelgeving en het beschermen tegen cyberdreigingen in diverse sectoren, zoals de gezondheidszorg en de financiële sector. Prioriteit geven aan digitale hygiëne is essentieel voor organisaties die risico's willen beperken, vertrouwen willen opbouwen en duurzame groei en succes willen stimuleren in het digitale landschap van vandaag.

Unit 4 – 1 good practice van startups

Om effectieve identificatie van bedreigingen en preventieve maatregelen te illustreren, gaan we dieper in op een voorbeeld waarin de nadruk ligt op cyberbeveiligingstraining voor personeelsleden. Dit voorbeeld onderstreept de cruciale rol van de opleiding van werknemers bij het versterken van digitale beveiligingsmaatregelen.

CyberSec Europa

Context

CyberSec Europe is een startup op het gebied van cyberbeveiliging gevestigd in Berlijn, Duitsland, gespecialiseerd in het leveren van beveiligingsoplossingen voor kleine en middelgrote ondernemingen (KMO's). CyberSec Europe, opgericht in 2017, heeft zich snel gevestigd als een vertrouwde leverancier van cyberbeveiligingsdiensten op de Europese markt. Naarmate het bedrijf groeide en zijn klantenbestand uitbreidde, erkende het het cruciale belang van cyberbeveiligingseducatie voor zijn werknemers.

Ondanks het feit dat CyberSec Europe een team van bekwame cyberbeveiligingsprofessionals heeft, heeft het vastgesteld dat het nodig is om het bewustzijn van zijn werknemers over best practices op het gebied van cyberbeveiliging te vergroten. Met de toenemende verfijning van cyberdreigingen en de invoering van regelingen voor werken op afstand, nam het risico op beveiligingsincidenten zoals phishing-aanvallen en datalekken toe. CyberSec Europe begreep dat het opleiden van zijn werknemers over cyberbeveiligingsrisico's en -protocollen essentieel was om zijn reputatie als betrouwbare cyberbeveiligingsprovider te behouden.

Oplossing

CyberSec Europe implementeerde een uitgebreid beveiligingstrainingsprogramma voor alle medewerkers, gericht op belangrijke gebieden zoals het detecteren van bedreigingen, het reageren op incidenten en

naleving van gegevensbeschermingsvoorschriften zoals de Algemene Verordening Gegevensbescherming (AVG). Het trainingsprogramma is ontworpen om interactief en boeiend te zijn en afgestemd op de specifieke behoeften van het personeel van CyberSec Europe.

Het beveiligingstrainingsprogramma werd gedurende drie maanden bedrijfsbreed uitgerold. Het bestond uit een reeks workshops, webinars en hands-on oefeningen onder leiding van interne cybersecurity-experts en externe consultants. Onderwerpen die in het trainingsprogramma aan bod kwamen, waren onder meer:

- ✓ Phishing-e-mails herkennen en erop reageren
- ✓ Sterke wachtwoorden maken en beheren
- ✓ Veelvoorkomende tekenen van cyberaanvallen herkennen
- ✓ Gevoelige gegevens beschermen en naleving van de AVG waarborgen
- ✓ Het melden van beveiligingsincidenten en het volgen van procedures voor incidentrespons.

Om deelname en betrokkenheid aan te moedigen, stimuleerde CyberSec Europe werknemers om de trainingsmodules te voltooien en bood het beloningen aan voor voorbeeldige prestaties bij beveiligingsbewustzijnsoefeningen. Het bedrijf bood ook doorlopende ondersteuning en middelen aan werknemers, zoals toegang tot cyberbeveiligingstools en online bronnen.

De implementatie van regelmatige beveiligingstrainingen leverde positieve resultaten op voor CyberSec Europe:

1. Verhoogd veiligheidsbewustzijn. Medewerkers werden waakzamer en beter geïnformeerd over cyberbeveiligingsrisico's, wat leidde tot een vermindering van beveiligingsincidenten en datalekken.

2. Verbeterde beveiligingspraktijken. Werknemers hebben best practices op het gebied van cyberbeveiliging toegepast, zoals het gebruik van sterke wachtwoorden, het versleutelen van gevoelige gegevens en het onmiddellijk melden van verdachte activiteiten.

3. Verbeterd vertrouwen van de klant. De toewijding van CyberSec Europe aan cyberbeveiligingseducatie toonde zijn toewijding aan het beschermen van klantgegevens en privacy, waardoor het vertrouwen en de geloofwaardigheid van zijn klanten worden vergroot.

4. Gereedheid voor naleving. Door werknemers voor te lichten over GDPR-vereisten en andere regelgevende normen, heeft CyberSec Europe zijn nalevingshouding verbeterd en het risico op boetes van regelgevende instanties geminimaliseerd.

CyberSec Europe's proactieve benadering van cybersecurity-educatie onderstreept het belang van regelmatige beveiligingstrainingen voor startups in Europa. Door te investeren in het bewustzijn en de empowerment van werknemers, kon CyberSec Europe zijn cyberbeveiliging versterken, risico's beperken en

vertrouwen opbouwen bij zijn klanten. Dit praktijkvoorbeeld benadrukt de effectiviteit van beveiligingstraining bij het verbeteren van digitale hygiëne en het beschermen van startups tegen cyberdreigingen op de Europese markt.

Het waarborgen van goede digitale hygiënepraktijken is van cruciaal belang voor startups in Europa om te gedijen in het digitale landschap van vandaag. De toenemende prevalentie van cyberdreigingen, datalekken en wettelijke vereisten onderstreept het belang van het prioriteren van inspanningen op het gebied van cyberbeveiliging, gegevensbescherming en naleving. Door robuuste digitale hygiënemaatregelen te implementeren, kunnen startups hun digitale activa beschermen, gevoelige gegevens beschermen en vertrouwen opbouwen bij klanten, partners en belanghebbenden. Het bereiken en behouden van een goede digitale hygiëne vereist echter een gezamenlijke inspanning, voortdurende waakzaamheid en een streven naar continue verbetering.

Aanbevelingen voor het verbeteren van de digitale hygiëne van start-ups in Europa

- ✓ Het wordt aanbevolen dat startups regelmatig beoordelingen uitvoeren van hun digitale hygiënepraktijken, waaronder cyberbeveiligingshouding, protocollen voor gegevensbeheer en de nalevingsstatus van de regelgeving. Dit zal helpen bij het identificeren van kwetsbaarheden, hiaten en verbeterpunten.
- ✓ Op basis van de bevindingen van de beoordeling is het raadzaam voor startups om uitgebreide digitale hygiënestrategieën te ontwikkelen die zijn afgestemd op hun specifieke behoeften, doelen en risicoprofielen. Strategieën moeten betrekking hebben op belangrijke gebieden zoals cyberbeveiliging, gegevensbescherming, naleving en respons op incidenten.
- ✓ Het wordt aanbevolen dat startups investeren in cyberbeveiligingstechnologieën en -oplossingen om hun digitale infrastructuur te beschermen tegen cyberdreigingen, malware en datalekken. Dit kunnen firewalls, antivirussoftware, versleutelingstechnologieën en inbraakdetectiesystemen zijn.
- ✓ Startups moeten prioriteit geven aan gegevensbescherming en privacy door robuuste protocollen voor gegevensbeheer te implementeren, waaronder codering, toegangscontroles en mechanismen voor gegevensback-up en -herstel. Naleving van regelgeving zoals de AVG is essentieel voor startups die met persoonsgegevens omgaan.
- ✓ Het is raadzaam voor startups om het bewustzijn en de educatie van cyberbeveiliging onder werknemers te bevorderen om ervoor te zorgen dat ze potentiële risico's, best practices en procedures voor het handhaven van een goede digitale hygiëne begrijpen. Regelmatige trainingssessies, bewustmakingscampagnes en phishing-simulaties kunnen helpen het bewustzijn van cyberbeveiliging te versterken.

✓ Startups moeten incidentresponsplannen ontwikkelen en implementeren om effectief te reageren op cyberbeveiligingsincidenten, datalekken of andere noodsituaties. Plannen moeten rollen, verantwoordelijkheden en procedures schetsen voor het opsporen, beheersen en beperken van incidenten.

✓ Continue monitoring en evaluatie zijn essentieel voor het handhaven van een goede digitale hygiëne. Het wordt aanbevolen dat startups regelmatig de effectiviteit van hun digitale hygiënemaatregelen beoordelen, audits en beoordelingen uitvoeren en de nodige aanpassingen maken om opkomende bedreigingen en uitdagingen aan te pakken.

✓ Startups moeten op de hoogte blijven van de nieuwste cyberbeveiligingsbedreigingen, trends en regelgeving die van invloed zijn op hun branche. Door regelmatig nieuws over cyberbeveiliging te monitoren, deel te nemen aan brancheforums en samen te werken met cyberbeveiligingsprofessionals, kunnen startups de evoluerende bedreigingen en risico's voorblijven.

Kortom, het verbeteren van digitale hygiënepraktijken is essentieel voor startups in Europa om hun digitale activa te beschermen, risico's te beperken en het vertrouwen van belanghebbenden te behouden. Door alomvattende strategieën te implementeren, te investeren in cyberbeveiligingstechnologieën, bewustzijn te bevorderen en voortdurend toezicht te houden op en zich aan te passen aan veranderende bedreigingen, kunnen startups hun digitale veerkracht versterken en gedijen in een concurrerend landschap.

Kernpunten

- Het wordt aanbevolen dat startups prioriteit geven aan cyberbeveiligingseducatie voor hun werknemers om bewustzijn te vergroten en hen in staat te stellen cyberdreigingen effectief te herkennen en erop te reageren. Trainingsprogramma's moeten onderwerpen behandelen zoals phishing-bewustzijn, wachtwoordbeheer en protocollen voor incidentrespons.
- Het vaststellen van robuuste beleidslijnen en procedures voor digitale hygiëne is essentieel voor het bevorderen van een cultuur van cyberbeveiliging binnen startups. Het is raadzaam om beleid te ontwikkelen

dat betrekking heeft op gebieden zoals de complexiteit van wachtwoorden, software-updates, toegangscontroles en voorschriften voor gegevensbescherming.

- Regelmatige audits en handhavingsmechanismen helpen bij het waarborgen van naleving en verantwoording binnen startups. Het wordt aanbevolen om regelmatig audits uit te voeren en handhavingsmechanismen in te voeren om de naleving van digitale hygiënebeleidslijnen en -procedures te monitoren.
- Startups moeten investeren in technologische oplossingen om hun digitale hygiënepraktijken te verbeteren. Dit omvat het inzetten van cyberbeveiligingstools zoals multi-factor authenticatie, coderingstechnologieën, endpoint-beveiligingssoftware en netwerkbewakingstools om de verdediging tegen cyberdreigingen te versterken.
- Naleving van wettelijke vereisten en industrienormen is van cruciaal belang voor startups om hun toewijding aan ethische bedrijfspraktijken te tonen en zich te beschermen tegen juridische en financiële gevolgen. Startups moeten zich houden aan regelgeving zoals GDPR, HIPAA, PCI DSS of SOX om de privacy, beveiliging en integriteit van gegevens te waarborgen.
- Het concept van digitale hygiëne integreert inzichten uit verschillende disciplines, waaronder cybersecurity, informatiemanagement, menselijke factoren, organisatiegedrag en compliance-theorie. Door gebruik te maken van deze perspectieven kunnen startups benaderingen ontwikkelen om de complexe uitdagingen van cyberbeveiliging en gegevensbescherming effectief aan te pakken.

Verwijzingen:

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

Module 2 - Digitale hygiënetools en integratie in dagelijkse routines

Unit 1- Top digitale hygiënetools voor startups

Een onderling verbonden wereld brengt risico's met zich mee van bredere en complexere digitale bedreigingen. Daarom is het belangrijker dan ooit dat start-ups veel belang hechten aan cybersecurity om hun waardevolle activa en vertrouwelijke informatie te beschermen. In deze module leert u over enkele van de belangrijkste strategieën en praktijken die start-ups zouden moeten ondernemen om hun online beveiliging te verbeteren. Deze variëren van het maken van sterke wachtwoorden tot het implementeren van grondige oplossingen voor gegevensback-up. Deze gids biedt u de kennis en tools die start-ups moeten kennen om online veilig te blijven. Deze unit neemt u mee door de belangrijkste principes en geeft een reeks aanbevelingen die u zullen helpen een sterke basis te leggen voor uw digitale hygiënestrategie en uw digitale activa effectief te beschermen.

Een goede wachtwoordhygiëne handhaven: de basis

Ticketmaster werd in januari 2021 aangeklaagd voor het hacken van de computersystemen van een rivaliserend bedrijf nadat een ex-werknemer van het rivaliserende bedrijf zijn/haar inloggegevens had gebruikt om Ticketmaster stiekem toegang te geven tot de computers van zijn concurrent. Waarnemend procureur DuCharme verklaarde dat "Ticketmaster-medewerkers bij talloze gelegenheden illegaal toegang hebben gekregen tot de computers van een concurrent zonder toestemming om zakelijke kennis te stelen via onrechtmatig verkregen wachtwoorden". Deze singulariteit van de zaak leidde ertoe dat Ticketmaster werd onderworpen aan een contante boete van $ 10 miljoen onder de voorwaarden van de Computer Fraud and Abuse Act. (Jones, 2022)Google Cloud's 2023 Threat Horizons-rapport geeft aan dat 86% van de inbreuken op de beveiliging het gebruik van gestolen inloggegevens omvat, en dat problemen met inloggegevens verantwoordelijk zijn voor meer dan 60% van de onderliggende oorzaken van de inbreuken - problemen die sterkere flanken voor identiteitsbeheer van de organisatie zouden kunnen helpen oplossen. Volgens (Keszthely, 2013) kan het nemen van het wachtwoord van iemand anders op vier basismanieren worden voltooid:

1- Standaardwoorden: Computers en applicaties hebben standaardwachtwoorden ingebouwd. Computer- en accountwachtwoorden kunnen ongeldig zijn of deel uitmaken van een afzonderlijke reeks veelgebruikte woorden zoals '123456', 'asdfgh' en 'wachtwoord'.

2- Verband tussen inlognaam en wachtwoorden: Het raden van wachtwoorden of logica is wanneer de aanvallers de tijd nemen om systematisch de gebruikersnaam en het wachtwoord te raden. De gebruiker kan de aanvaller zelfs helpen de gebruikersnaam en het wachtwoord te raden. Enkele voorbeelden zijn "password", "login-login", "qwerty" en "letmein".

3- Methode van het woordenboek: Hackers verzamelen enkele algemene wachtwoorden en selecteren deze uit de lijst. Ze zullen ze een voor een downloaden omdat de tools offline werken en meer kans van slagen hebben als ze langzamer werken. Bovendien hebben ze nog steeds de mogelijkheid om elke streng te testen zonder internetverbinding.

Om schade door wachtwoorddiefstal te voorkomen, is het noodzakelijk om prioriteit te geven aan de selectie van sterke, veilige wachtwoorden. Stel enkele aanbevolen tips voor het maken van sterke wachtwoorden voor:(Kato & Klyuev, 2013)

- **Gebruik hoofdletters en interpunctie**: Gebruik hoofdletters en leestekens om een sterker wachtwoord te maken.
- **Mix It Up:** Integreer zowel letters als cijfers om veiligere wachtwoorden te genereren.
- **Vermijd algemene informatie**: Gebruik geen gemakkelijk te raden woorden en persoonlijke informatiegegevens in wachtwoorden.
- **Overweeg langere wachtwoorden:** Streef naar langere wachtwoorden die u gemakkelijk kunt onthouden.
- **Gebruik wachtwoordmanagers**: Gebruik programma's die zijn ontworpen om wachtwoorden veilig op te slaan, zoals LastPass.
- **Unieke wachtwoorden**: Formuleer verschillende wachtwoorden voor verschillende accounts.

Naast het oefenen van veilige wachtwoordgewoonten als individu, moeten bedrijven beleid implementeren dat gericht is op het verbeteren van de wachtwoordbeveiliging. stelt voor dat op organisatieniveau de wachtwoordrichtlijnen zich moeten concentreren op de gebruiker. De richtsnoeren moeten de unieke vereisten en vaardigheden van de gebruikers in hun dagelijkse werk weerspiegelen. Organisaties kunnen de beveiliging maximaliseren en tegelijkertijd de effectiviteit en efficiëntie van gebruikers bij het beheren van wachtwoorden versterken door te voldoen aan de principes van mens-computerinteractie en rekening te houden met specifiek gebruik. Bovendien moeten bedrijven proberen strikte standaarden voor het maken van wachtwoorden te analyseren en toe te passen door gebruik te maken van nieuwe wachtwoordtechnieken en apparaten zoals Telepathwords. Bovendien moeten bedrijven ervoor zorgen dat ze werknemers helpen bij een preventieve inspanning om zwakke of beïnvloede wachtwoorden te gebruiken. Het overtreffen van het schema door middel van deze technieken zal de veiligheid aanzienlijk verbeteren. (Inglesant & Sasse, 2010)(Blocki & Liu, 2023)

Vitale infrastructuur beveiligen met tweefactorauthenticatie

Tweefactorauthenticatie (2FA) is een beveiligingsmaatregel waarbij gebruikers een secundaire component moeten verstrekken voor gebruikersbevestiging. Deze methode voegt een authenticatiefactor toe aan het wachtwoordverificatiesysteem. Er zijn enkele voordelen die een beoordelingsplatform zou hebben bij de implementatie van 2FA :(Tellini & Vargas, 2017)

- **Het elimineren van de mogelijkheid van ongeoorloofde toegang**: 2FA gaat verder dan alleen het gebruik van een gebruikersnaam en wachtwoord. Het maakt gebruik van een volledig apart systeem voor authenticatie, helemaal.
- **Bescherming tegen wachtwoorddiefstal:** Gebruikersnamen en wachtwoorden worden dagelijks gestolen. Met 2FA heeft een aanvaller meer nodig dan alleen de naam en het wachtwoord van de gebruiker om onwettige toegang te krijgen.
- **Verminderd risico op ongeoorloofde toegang**: Met 2FA is ongeoorloofde of onbewezen toegang minder waarschijnlijk vanwege de extra authenticatielaag die de hacker nodig zou hebben om toegang tot het account te voltooien en zou hij in het bezit moeten zijn van de telefoon van de gebruiker of een code die op zijn telefoon is gegenereerd.
- **Verhoogd gebruikersvertrouwen:** Het vertrouwen en vertrouwen in het platform kan toenemen wanneer gebruikers weten dat hun account wordt beschermd door meer dan alleen een wachtwoord.
- **Naleving van beveiligingsnormen:** Het gebruik van 2FA kan ervoor zorgen dat uw aanmeldingen voldoen aan best practices voor online beveiliging en mogelijk vereist zijn door specifieke regelgeving of normen in uw branche.
- **Beperking van veelvoorkomende wachtwoordproblemen:** 2FA helpt bij het verminderen van veelvoorkomende wachtwoordproblemen, zoals slechte wachtwoordkeuzes en hergebruik. Door minder afhankelijk te zijn van één wachtwoord, kan 2FA ons helpen complexere wachtwoorden te gebruiken.

2FA is een tweestapsverificatieproces waarbij gebruikers twee verschillende soorten authenticatiefactoren moeten opgeven voordat ze toegang verlenen aan de eindgebruiker. De drie soorten factoren zijn iets dat de gebruiker weet (kennisfactor), iets dat de gebruiker heeft (bezitsfactor) en iets wat de gebruiker is (inherentiefactor). De tweefactorauthenticatiemethode maakt wachtwoordgerichte authenticatietechnieken veiliger. Services kunnen dynamische combinaties van factoren gebruiken om de zekerheid van gebruikersreferenties aanzienlijk te vergroten door de risico's en voordelen te kwantificeren.(De Cristofaro, Du, Freudiger, & Norcie, 2013) (Han, Sun, Shen, Chang, & Shen, 2013)

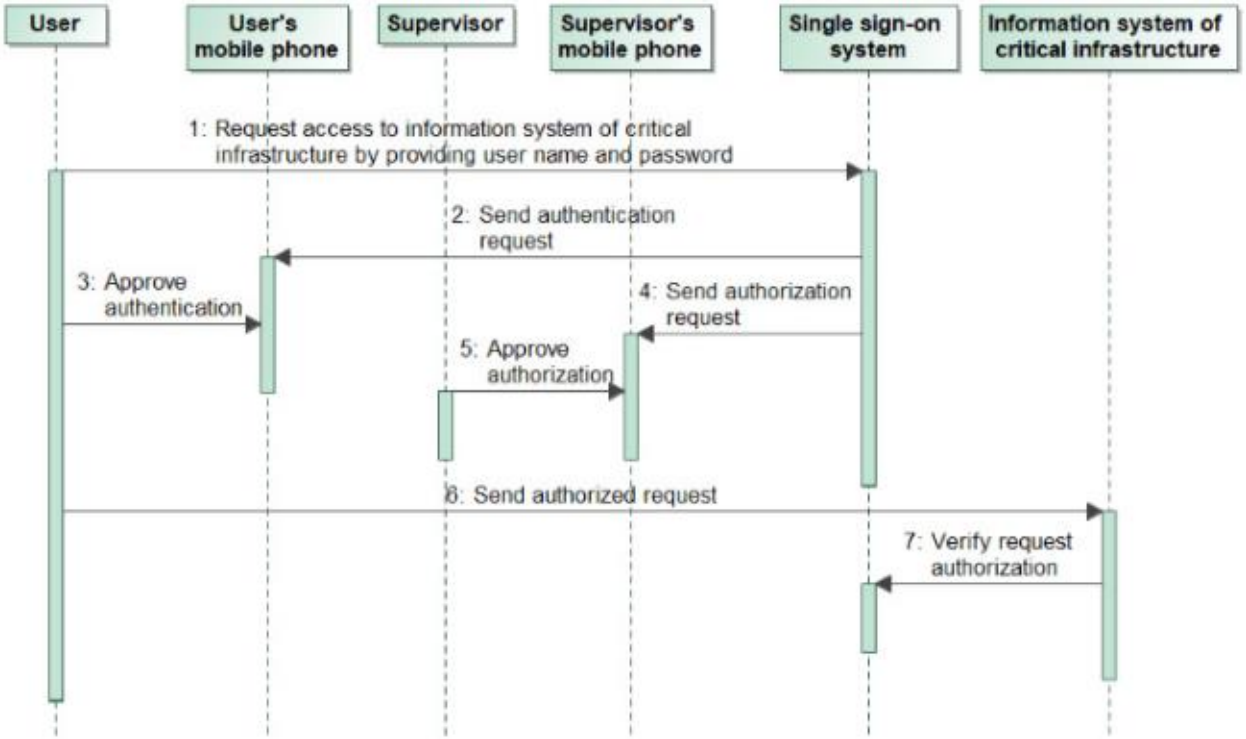
Tabel 1: Enkele klassen van authenticatiefactoren

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

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

(Bruzgiene & Jurgilas, 2019) Biedt een verificatiemethode die werkt in een proces in drie stappen voor het beveiligen van externe toegang tot kritieke infrastructuurinformatiesystemen. Eerst voert de gebruiker zijn/haar account-ID en wachtwoord in. Zodra de juiste informatie is ingevoerd, wordt een authenticatieverzoek van de lokale veiligheidsautoriteit (LSA) naar het mobiele apparaat van de gebruiker gestuurd. Vervolgens moet de gebruiker het verzoek goedkeuren door een enkele aanraking op het scherm van de telefoon; Hierdoor kan het mobiele apparaat een autorisatieverzoek sturen naar de supervisor(s) van de gebruiker om het niveau van toegangsrechten voor het externe systeem te bepalen. Zodra de gebruikersaanvraag met succes is goedgekeurd door de supervisor(s), krijgt de aanvragende gebruiker toegangsrechten tot het externe systeem

Figuur 1: De voorgestelde authenticatiemethode door (Bruzgiene & Jurgilas, 2019)



Bron : (Bruzgiene & Jurgilas, 2019)

Tijdige software-updates: versterking van de systeembeveiliging

Software-updates zijn erg belangrijk omdat ze fouten oplossen of de prestaties van software, zoals stuurprogramma's en besturingssystemen, verbeteren. Door de software bij te werken, zorgt u ervoor dat deze compatibel is met andere software- en hardwaresystemen en houdt u uw systemen veilig en beveiligd door de nieuwste versie van de software uit te voeren. De updates omvatten beveiligingsupdates die nodig zijn om een computer te beschermen tegen schadelijke software en kwetsbaarheden, functie-updates die variëren in termen van ernst, aangezien ze alles kunnen omvatten, van kleine bugfixes tot belangrijke workflowwijzigingen, en de cumulatieve update die de installatie van alle eerdere updates vereist voordat de nieuwste update wordt bereikt. Deze verbeteringen helpen de veiligheid en functionaliteit van softwaresystemen te behouden. Het is om deze reden belangrijk om ervoor te zorgen dat u op de hoogte bent van alle noodzakelijke updates. (Mathur, Malkin, Harbach, Péer, & Egelman, 2018)(Vaniea, Rader, & Wash, 2014)

Veel gebruikers hebben echter de neiging om het updaten van hun software te vermijden vanwege waargenomen factoren. Deze factoren omvatten *Update Kosten*, zoals de tijd die nodig is om te installeren,

waarbij opnieuw moet worden opgestart en de gebruikte schijfruimte; *Update noodzaak*, met inbegrip van de tevredenheid van de gebruiker over het huidige systeem, de duidelijkheid van de redenen voor de update en het belang van de update die door de gebruiker wordt ervaren en *Risico bijwerken* die zorgen met zich meebrengen over gegevensverlies tijdens updates en dat elke update een virus of malware kan bevatten die een systeem kwetsbaar kan maken . Het nalaten van het upgraden van software kan computersystemen vatbaar maken voor de acties van hackers die kunnen proberen de computers te infecteren met nieuwe virussen en wormen. Het kan ook ernstige gevolgen hebben voor uw computers. Niet-gepatchte beveiligingsfouten zullen het systeem niet alleen minder veilig maken, maar ze zijn ook de reden waarom de meeste virussen zo succesvol zijn. (Mathur, Malkin, Harbach, Péer, & Egelman, 2018)

Een beleid voor de levering van software-updates is een beleid dat is ontwikkeld door organisaties en die tijdlijnen en methoden definiëren voor het beoordelen en leveren van beveiligingsgerelateerde software-updates. Dit beleid is gericht op de onmiddellijke levering van beveiligingsupdates, binnen een beperkt tijdsinterval (beperking) om het beveiligingslekvenster te minimaliseren, als de beperking dit toestaat. Organisaties kunnen een meer strategische aanpak hanteren, afhankelijk van de beperkingen van de middelen. Innovatieve oplossingen kunnen bijvoorbeeld bestaan uit peer-to-peer op blockchain gebaseerde systemen en grootschalige overlay-netwerken, om de zeer efficiënte en doelmatige distributie van beveiligingsupdates naar brede netwerken van eindgebruikers mogelijk te maken. . Het beleid is om verschillende categorieën patches en de bijbehorende tijdlijnen voor beoordeling en levering op te splitsen om ervoor te zorgen dat updates, op verschillende niveaus, worden beoordeeld in overeenstemming met hun behoefte, kosten en bijbehorende risico's, voordat ze worden geïmplementeerd.(Mugarza, Flores, & Montero, 2020)

Dit zijn de suggesties voor software-updates voor bedrijven[1]:

- **Tijdige installatie:** Door beveiligingsupdates op tijd te installeren, kunt u uw systemen beschermen tegen kwetsbaarheden en bedreigingen.
- **Duidelijke communicatie:** Gebruikers zijn vaak resistent tegen updates omdat ze niet begrijpen waarom je ze nodig hebt. Het is belangrijk om te communiceren waarom de update belangrijk is en dat het niet zomaar een willekeurige patch is die door de leverancier wordt geleverd. Het is ook nuttig om in uw e-mail te vermelden dat sommige updates patches zijn voor beveiligingslekken die mogelijk al zijn uitgebuit
- **Minimaliseer onderbreking:** Schakel stille installaties of configuraties van het systeem in, waardoor het gemakkelijker wordt om updates toe te passen. Een andere manier om onderbrekingen tot een minimum te beperken, is door updates te distribueren en te implementeren tijdens daluren.

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

- **Gebruikerseducatie:** Eindgebruikers voorlichten over het belang van software-updates voor het handhaven van systeembeveiliging en -functionaliteit om proactief updategedrag te bevorderen
- **Testprocedures:** Verbeter de testprocedures om ervoor te zorgen dat updates grondig worden getest op compatibiliteit en mogelijke risico's voordat ze worden geïmplementeerd.
- **Onderscheid maken tussen updates:** Maak onderscheid tussen beveiligingsupdates en functie-updates, zodat gebruikers de waarde van elk type update begrijpen en deze dienovereenkomstig prioriteren.
- **Cumulatieve updates:** Overweeg de implicaties van cumulatieve updates en moedig de gebruiker aan om de kritieke beveiligingspatches te installeren.

Antivirusbescherming: de integriteit van het systeem waarborgen

Volgens is antivirussoftware een gespecialiseerd programma dat het besturingssysteem beschermt tegen virussen, spyware, hackeraanvallen en andere ongeoorloofde computertoegang om te voorkomen dat waardevolle persoonlijke gegevens worden gestolen, of de ongeautoriseerde controle van de computer is een andere computertoepassing (freeware, shareware en commercieel). Antivirussoftware wordt gebruikt om computervirussen te detecteren die betrekking kunnen hebben op computerbestanden, toepassingsprogramma's en de besturingssystemen van de computer. Om deze reden kan het ook worden ingesteld om regelmatig beoordelingen van de bestanden en het geheugen van de computer uit te voeren, om elke bekende virushandtekening te detecteren en zo mogelijke besmetting van het computersysteem en zijn bestanden te voorkomen. Het is belangrijk om de antivirussoftware regelmatig bij te werken met de nieuwste definities en virushandtekeningen, omdat er regelmatig nieuwe virussen en variaties op de markt komen. Door de nieuwste virusbedreigingen te detecteren, biedt het bijwerken van de antivirussoftware een robuuste verdediging tegen de constante evolutie van computerbedreigingen terwijl het werkt. (Rohith & Kaur, 2021)(Naie & Teymournejad, 2012)

Er zijn verschillende tekenen die verband houden met de aanwezigheid van computervirussen op uw computer, waarvan er hieronder enkele worden beschreven. Elk van deze symptomen kan duiden op een virusprobleem. Daarom is het erg belangrijk om het systeem zo snel mogelijk te scannen met antivirussoftware :(Kumar, 2008)

- Langzamere computer
- Basistaken duren langer
- Vastlopen en crashen
- Constante schijfactiviteit
- Overmatig CPU-gebruik
- Surfen op internet is veel langzamer dan voorheen.
- Toepassingen worden niet gestart.
- Pop-ups en ongenode berichten met inhoud voor volwassenen.
- Harde schijven potloodnummers.
- Openen en sluiten van het cd-rom-station.

Als u onverwacht een of meer van deze situaties tegenkomt, neem dan contact op met uw IT-beheerder of voer de nodige viruscontroles uit. Het is belangrijk op te merken dat het van cruciaal belang is om een antivirusprogramma op alle systemen te installeren, zelfs als het niet de beste is. Dit helpt om een hogere moeilijkheidsgraad te geven aan aanvallers die proberen de beveiliging van een systeem in gevaar te brengen. Moving Ahead biedt waardevolle inzichten in de uitdagingen en overwegingen die moeten worden onderzocht bij de selectie van antivirussoftware voor een organisatie: (Min & Varadharajan, 2015)(Ncube & Maiden, 2004)

1. Gebruik een vragenlijst in combinatie met andere elicitatietechnieken

2. Zorg ervoor dat de vragen kort zijn en zo goed dat ze goede antwoorden krijgen van leveranciers.

3. Vraag om documentatie met antwoorden op de vragenlijst, zodat we de productbeschrijving beter kunnen afstemmen op het daadwerkelijke product.

4. Definieer duidelijk wat u zegt in het product en hoe ver u gaat testen, zodat u de testcase beter kunt definiëren.

5. Begrijp dat we in de loop van de tijd beperkt zullen zijn bij het selecteren van COT-software en kijk naar sjablonen voor procesbeschrijvingen om bij verschillende gelegenheden sneller te zijn.

6. Weet dat je niet alles kunt testen. Sommige vereisten kunnen beperkingen hebben.

Gegevensback-ups: een schild tegen verlies

Hoewel onvoorzien, kunnen onverwachte gebeurtenissen en cyberincidenten een aanzienlijke hoeveelheid schade aanrichten aan de gegevens van een organisatie. Dit is waar gegevensback-ups in het spel komen. Gegevensback-ups zijn een cruciaal onderdeel van cyberbeveiliging en het onderhouden van een veilige digitale omgeving. Gegevensback-ups kunnen een geweldig hulpmiddel zijn voor organisaties in geval van inbreuken op de beveiliging. Samen met de bescherming van gegevens tegen verlies, bieden back-upsystemen de mogelijkheid om de eerdere versies van bestanden te herstellen, zodat de bestandsgeschiedenis wordt beschermd. De meeste back-uptools kunnen meerdere exemplaren van hetzelfde bestand in vele formaten bewaren, elk gekoppeld aan een tijdstempel. Ook compressie en versleuteling zijn gemeenschappelijke kenmerken van bijna alle back-upsystemen. Compressie helpt gebruikers bij het overbrengen van bestanden via een netwerk of internet wanneer ze worden gedeeld. (Sampaio & Bernardino, 2015)

Technieken van gegevensback-upsystemen omvatten volledige back-up waarbij een volledige kopie van alle gegevens wordt gemaakt, differentiële back-up die gegevenswijzigingen sinds de laatste volledige back-up opslaat, en incrementele back-up die alleen de gegevensdelen opslaat die zijn gewijzigd sinds de vorige back-

up is gemaakt. . Elke methode heeft andere gevolgen en is geschikt voor back-upoperaties. Betrouwbare back-ups zijn opmerkelijk omdat sommige gegevens van onschatbare waarde zijn en het opnieuw maken van extra gegevens tijdrovend is/geldverslindend. Back-up van gegevens is niet alleen om gegevensverlies te voorkomen, maar ook om een oude versie te herstellen. Deze dubbele functionaliteit is belangrijk voor zowel gegevensherstel als voor de naleving van bepaalde wettelijke normen. Hier volgen enkele praktische tips voor back-ups van kleine bedrijven: (Nadee & Somwang, 2021) (Traeger, Joukov, Sipek, & Zadok, 2006) (Sampaio & Bernardino, 2015) (Rock, 2023)

Strategie voor gegevensbescherming: Kleine bedrijven moeten een gedetailleerd plan voor gegevensbescherming ontwerpen, dat deel zal uitmaken van hun BCP (Business Continuity Plan) of DRP (Disaster Recovery Plan).

Back-upoplossingen: Bedrijven moeten geen eenvoudige back-upoplossingen gebruiken, maar eerder een aantal robuuste BC/DR-oplossingen (Business Continuity /Disaster Recovery) kiezen, die een minimale operationele onderbreking garanderen.

Back-upfrequentie en opslag: Regelmatige back-ups zijn essentieel en moderne back-upoplossingen maken regelmatig back-ups. Het wordt aanbevolen om hybride back-upbescherming te hebben, die gegevens zowel ter plaatse als in de cloud opslaat.

Beveiliging en naleving: Het is belangrijk om de back-ups te beschermen tegen cyberaanvallen en ook te voldoen aan het beleid voor het bewaren van gegevens. Het versleutelen van back-ups tijdens het transport en in rust zou een extra beveiliging zijn.

Back-upgegevens op beveiligde apparaten: Configureer back-upapparaten alleen voor uitgaande communicatie binnen een beveiligd lokaal netwerk. Deze aanpak helpt voorkomen dat een cybercrimineel de controle over uw back-ups overneemt.

Back-upgegevens op afzonderlijke apparaten: Zorg ervoor dat u back-upapparaten gescheiden houdt van het lokale netwerk om te voorkomen dat back-ups worden beïnvloed wanneer ransomware optreedt op het lokale netwerk. Een van de voordelen van het maken van back-ups van gegevens in de cloud is dat dit kan worden gedaan vanaf elke verbonden plaats, weg van de kantoren van de hoofdorganisatie.

Gebruik versleutelde back-ups: Gebruik versleutelde opslag en overdracht om kritieke gegevens te beschermen tegen ongeoorloofde toegang, manipulatie en corruptie.

Maak een back-up van alle eindpuntgegevens met behulp van herstelsoftware: Een zeer belangrijke bron van gegevensverlies is verloren, gestolen of beschadigde laptops/desktops. Als gevolg hiervan kunt u geen back-up maken van de verloren gegevens of deze herstellen. Wetende dat back-upapparaten de vorm aannemen

van desktops en servers, moet u altijd hersteloplossingen selecteren om alle gegevens op elke computer te beschermen en dienovereenkomstig eindpuntback-up selecteren.

Guardians Against Malicious Code: inzicht in anti-malwareoplossingen

Kwaadaardige uitvoerbare bestanden zijn niet-geautoriseerde programma's die zijn gemaakt om een computersysteem te besmetten of te beschadigen, wat een groot gevaar vormt voor de beveiliging van de computer. Gebruikers zijn meestal het slachtoffer van kwaadaardige software zonder het te weten. Het is het programma dat zonder medeweten op de achtergrond op de computer van een gebruiker wordt uitgevoerd en dingen doet zoals informatie stelen, virussen die uw apparaten schoonvegen of Trojaanse paarden die uw bestanden al dan niet verwijderen. Spyware, virussen, wormen, Trojaanse paarden, ransomware en adware zijn de meest voorkomende versies van malware. Elk bedrijf zou meer dan eens per dag een back-up van zijn systemen moeten maken en een robuuste anti-malware-oplossing moeten gebruiken. Bij het kiezen van anti-malwaresoftware voor een bedrijf moet met verschillende factoren rekening worden gehouden om ervoor te zorgen dat de oplossing past bij de behoeften of doelen van de organisatie: (Ye, Wang, Lİ, & Ye, 2007)(Alharbi, Alzahrani, Asseri, & Taramisi, 2020)

Beveiligingsfuncties: Realtime toegang, firewallbescherming en inbraakdetectie zijn belangrijke beveiligingsfuncties die moeten worden opgenomen in een anti-malwareprogramma. Deze functies zijn essentieel voor effectief bedreigingsbeheer en om ervoor te zorgen dat er geen bedreigingen zijn die over het hoofd worden gezien.

Operationele kenmerken: Operationele kenmerken van anti-malwaresoftware waar u op moet letten, zijn onder meer hoe gemakkelijk het is om de software te implementeren en te gebruiken, welke beheermogelijkheden de software heeft en hoe deze zal integreren met uw bestaande systemen.

Efficiëntie: Evalueer de efficiëntie van de anti-malwaresoftware bij het detecteren en verwijderen van schadelijke software. Zoek naar oplossingen met een hoog detectiepercentage tot 100% en een minimaal percentage fout-positieven.

Schaalbaarheid: Kies een oplossing die kan meegroeien met de behoeften van het bedrijf naarmate het groeit. Zorg ervoor dat de anti-malwaresoftwareoplossing kan voldoen aan de huidige behoeften van uw organisatie en aan toekomstige behoeften kan voldoen.

Controleer de reputatie van de leverancier: Een goede reputatie is een zeldzaam goed in de software-industrie, maar het is een van de meest waardevolle eigenschappen van elke softwareleverancier. Zoek naar leveranciers van anti-malware met een lange geschiedenis van hoogwaardige beveiligingsoplossingen. Zijn ze erkend door onafhankelijke testorganisaties?

Kosten: Het eerste waar u rekening mee moet houden, is de prijs van de anti-malwaresoftware. Verschillende leveranciers bieden hun software aan in verschillende prijsklassen en licentieopties, dus zorg ervoor dat het binnen uw budget valt. Sommige organisaties kunnen dit als een belangrijke factor classificeren, terwijl anderen dit als niet erg belangrijk beschouwen.

Ondersteuning en updates: Evalueer de staat van dienst van de leverancier op het gebied van ondersteuning en updates. Zoek een leverancier die regelmatig updates en technische ondersteuning biedt als er zich problemen voordoen.

Compatibiliteit is een van de dingen die een organisatie van een lijst moet afvinken, aangezien geen enkele software effectief kan zijn als u compatibiliteitsproblemen ondervindt. Compatibiliteitsproblemen zijn een van de grootste redenen waarom de software van een organisatie ineffectief wordt.

Unit 2 - Hoe maak je van digitale hygiëne een gewoonte bij het opstarten van operaties?

Het is van cruciaal belang om een cultuur te creëren op het gebied van cyberbeveiliging en cyberhygiëne in de dagelijkse bedrijfsvoering van een start-up. Cyberhygiënepraktijken zijn hetzelfde als persoonlijke hygiëne: ze bieden de nodige protocollen die moeten worden gevolgd om persoonlijke en bedrijfsgegevens/informatie veilig te houden. Start-ups, met hun gebrek aan geld, kunnen zich de tegenslagen van een cyberincident niet veroorloven. De zakelijke implicaties zijn niet beperkt tot alleen een financiële impact, maar omvatten verlies van klantvertrouwen, reputatieschade en mogelijke juridische gevolgen, die in een start-up het verschil kunnen betekenen tussen succesvol opschalen of voortijdig falen. Veel organisaties hebben nog steeds geen goed cyberhygiënegedrag, ook al is er veel gedaan om het cyberhygiëneprobleem aan te pakken. (Alkhaledi & Hawamdeh, 2023) (Kalhoro, Rehman, Ponnusamy, & Shaikh, 2021)

Goed gedrag op het gebied van cyberhygiëne is essentieel om cyberdreigingen en dagelijkse uitdagingen bij het aanpakken van cyberhygiëneproblemen te verminderen. Dit hoofdstuk dient om de strategieën te schetsen en uit te breiden die dagelijks worden toegepast voor startende bedrijven om een dagelijkse digitale hygiëneroutine te creëren.

2.1. De digitale gezondheid van uw startup beoordelen

Beoordeling van cyberbeveiligingsrisico's is een essentieel onderdeel van de bedrijfsplanning; Het omvat het identificeren, evalueren en inschatten van risico's voor de digitale activa en activiteiten van een organisatie. De toegepaste methode voor de beoordeling van cyberbeveiligingsrisico's stelt de organisatie in staat om haar beveiligingshoudingen te evalueren, waarde toe te kennen aan haar informatie en haar systemen, de

effectiviteit van haar huidige beveiligingsinfrastructuur en -activiteiten in te schatten en ook de omvang van de schade in te schatten die zou optreden als de specifieke risico's worden gerealiseerd. Door prioriteit te geven aan geïdentificeerde risico's, kunnen organisaties effectief middelen toewijzen om hun verdediging te versterken en de bedrijfscontinuïteit te waarborgen.

Talrijke onderzoeken bieden waardevolle bevindingen met betrekking tot de verschillende aspecten van de beoordeling van cyberbeveiligingsrisico's, die nuttig kunnen zijn in een bedrijf. wijst erop dat de beoordeling van de informatiebehoeften ook een van de belangrijkste stappen is in de richting van een doeltreffende afhandeling van afwijkingen in kmo's met behulp van digitale instrumenten. Het bepalen van de soorten informatie die moeten worden verzameld voor de procedures en het niveau van kriticiteit van de gegevens zal helpen om het risico van de integratie van de digitale systemen te minimaliseren. samengevat het risicobeoordelingsproces in de cyberbeveiliging van de luchtvaart, maar deze praktijken kunnen worden gebruikt als een algemeen kader bij risicobeoordeling in kmo's:(Chavez, ve diğerleri, 2020) (Elmarady & Rahouma, 2021)

1. Identificeer de systemen die bescherming nodig hebben. Met een goed begrip van waarvoor de systemen zijn gedefinieerd, klinkt het identificeren van de potentiële bedreigingen voor die systemen eenvoudig.

- Herken potentiële bedreigingen door de systemen te begrijpen.
- Definieer de grenzen van de te beoordelen systemen en beschrijf deze.

2. Maak een lijst van alle dingen die kunnen gebeuren om verlies of schade aan het systeem te veroorzaken. Begrijp wat er direct of indirect voor kan zorgen dat een beveiligingsdoelstelling niet wordt uitgevoerd en wat het verschil is tussen een dreiging en een kwetsbaarheid.

- Bepaal scenario's die het systeem direct of indirect kunnen schaden.
- Evalueer bedreigingen die de integriteit, vertrouwelijkheid en beschikbaarheid van het systeem kunnen beïnvloeden.

3. Beoordeel de waarschijnlijkheid en impact van bedreigingen. Bij het beoordelen van het zaad waarop een dreiging kan worden uitgevoerd, moeten veel factoren worden aangepakt.

- Evalueer de waarschijnlijkheid van bedreigingen.
- Beoordeel de potentiële impact van bedreigingen op veiligheid, efficiëntie, economie, politiek en het vertrouwen van het publiek.

4. Bepaal risiconiveaus. Beoordeel de risiconiveaus.

- Analyseer het risicoprofiel met behulp van waarschijnlijkheid, kwetsbaarheidsbeoordelingen en dreigingsimpact.

- Zet risiconiveaus om in kwalitatieve termen en bepaal de risicotolerantie.
- Categoriseer risiconiveaus met behulp van een gestandaardiseerde methodologie.

Implementeer risicobeperkende maatregelen die nodig zijn om risico's tot aanvaardbare niveaus te beperken. Door deze stappen te volgen, kunnen organisaties cyberbeveiligingsrisico's effectief beoordelen, bedreigingen identificeren en beleid implementeren om kritieke systemen te beschermen.

2.2. Totstandbrenging van een cultuur van digitale hygiëne

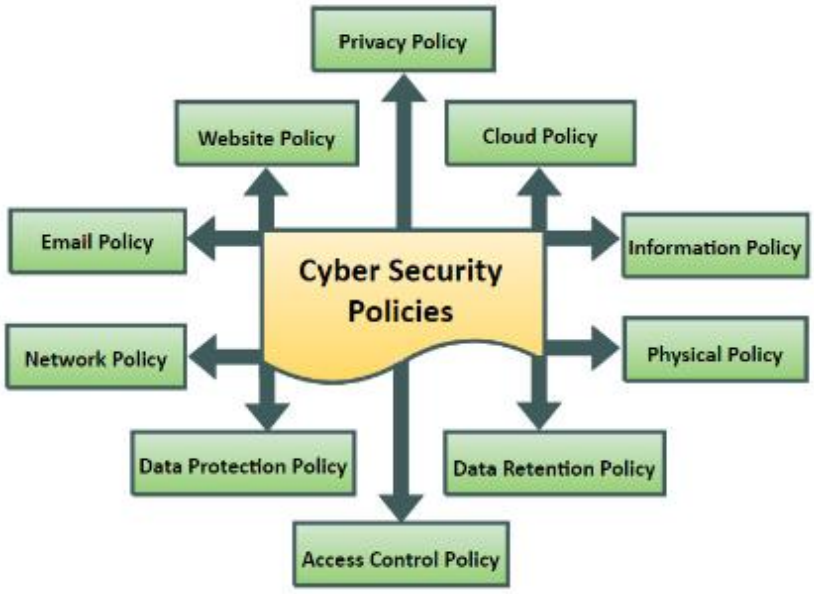
De cultuur van digitale hygiëne, het maken van een bloeiend digitaal ecosysteem, moet als eerste voorwaarde eerst worden ingebed in de organisatie. Dit moet top-down worden aangestuurd door het management. Het is niet alleen voldoende om over digitaal welzijn te praten, maar het moet ook in de praktijk worden gebracht door het topmanagement. Het begint met het ontwikkelen van beleid. Leiders moeten een alomvattend beleid aansturen en ontwikkelen dat gegevensbeheer regelt en de beveiliging verhoogt. Een regelmatige trainingssessie is zeer vereist. Het moet worden opgevat als een regulier programma om de werknemers bewust te maken van hoe ze veilig kunnen blijven en de nieuwste best practices op het gebied van digitale beveiliging. Open communicatie is van cruciaal belang. Het is erg belangrijk om een transparante cultuur te hebben in een organisatie waar werknemers zich op hun gemak voelen om te communiceren, hun zorgen kunnen uiten en ook kunnen melden als ze iets verdachts vinden dat beveiligingsproblemen zou kunnen veroorzaken. Dit is de enige manier waarop we kunnen zorgen voor een cultuur om digitale hygiëne en veiligheid te handhaven.

2.2.1. Beleidsontwikkeling

Het hebben van een sterk cyberbeveiligingsbeleid is erg belangrijk voor kleine en middelgrote ondernemingen (kmo's) om hun digitale activa te beveiligen en de operationele continuïteit te waarborgen. Onderzoek heeft aangetoond dat kmo's voor verschillende uitdagingen staan, waaronder het gebrek aan budget, de onbeschikbaarheid van specialisten en de toename van cyberdreigingen. Het hebben van cyberbeveiligingsmaatregelen kan ook datalekken aanzienlijk verminderen en de interne procesbeveiliging verbeteren, naast het bouwen van een betrouwbaar systeem met voldoende informatieverwerkingscapaciteit. Daarnaast kan de weerbaarheid van kmo's tegen cyberaanvallen worden verbeterd door middel van hun cyberbeveiligingsbeleid. de uitvoering van een holistische benadering van cyberweerbaarheid zou mkmo's beter in staat kunnen stellen om te anticiperen op een cyberaanval, deze op te sporen, te weerstaan, te herstellen, te herstellen en te evolueren na een cyberaanval. (Neri, Niccolini, & Martino, 2023)(Hasani, O'Reilly, Dehghantanha, Rezania, & Levallet, 2023)(Carias, Borges, Labaka, Arrizabalaga, & Hernantes, 2020)

Bedrijven moeten bij het ontwerpen van cyberbeveiligingsbeleid rekening houden met verschillende gebieden en cyberbeveiligingsbeleid op het juiste gebied opstellen op basis van hun behoeften. Om hun cyberbeveiligingsbeleid en -praktijken te bevorderen, kunnen verenigingen de onderdelen gebruiken om de taxonomie van cyberbeveiligingsbeleid te ontwikkelen. De componenten van de taxonomie van het cyberbeveiligingsbeleid die worden genoemd, worden geïllustreerd in figuur 2:(Mishra, Alzoubi, Gill, & Anwar, 2022)

Figuur 2: Taxonomie van cyberbeveiligingsbeleid



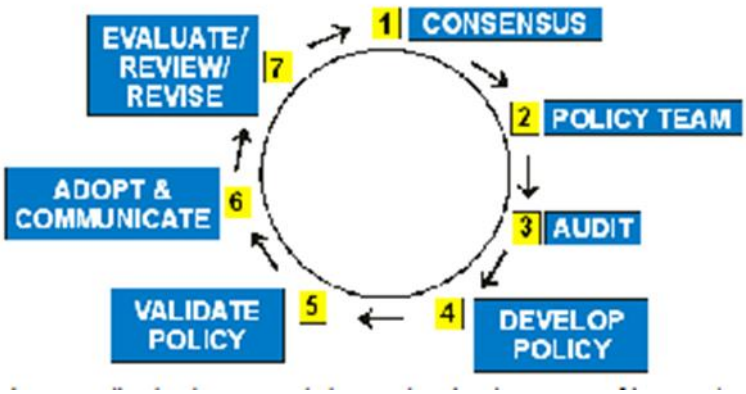
Bron: (Mishra, Alzoubi, Gill, & Anwar, 2022)

1. Privacybeleid: Richt zich op het beschermen van gevoelige persoonsgegevens en het waarborgen van de naleving van de regelgeving inzake gegevensbescherming.
2. Websitebeveiliging: Omvat het beveiligen van websites tegen cyberdreigingen en kwetsbaarheden om gebruikersgegevens te beschermen.
3. Beveiliging van cloud computing: Richt zich op beveiligingsmaatregelen voor cloudservices om gegevens die in de cloud zijn opgeslagen te beschermen.
4. E-mailbeveiliging: Richt zich op het beveiligen van e-mailcommunicatie en het voorkomen van e-mailgebaseerde cyberdreigingen.
5. Fysieke beveiliging: Omvat het beveiligen van fysieke toegang tot IT-infrastructuur en kritieke activa om ongeoorloofde toegang te voorkomen.
6. Netwerkbeveiliging: Richt zich op het beschermen van computernetwerken tegen cyberdreigingen en ongeoorloofde toegang.
7. Informatiebeveiliging: Omvat maatregelen om gevoelige informatie te beschermen
8. Toegangscontrole: Omvat het beheren van gebruikerstoegang tot systemen en gegevens om ongeoorloofde toegang te voorkomen.

9. Gegevensbewaring: Behandelt beleid voor het opslaan en beheren van gegevens gedurende de levenscyclus.
10.Gegevensbescherming: Richt zich op het beschermen van gegevens tegen verlies, diefstal of ongeoorloofde toegang door middel van versleuteling en beveiligingscontroles.

Zodra u de tekortkomingen en doelen kent, kunt u het cyberbeveiligingsbeleid ontwerpen om deze gebieden te bestrijken. Een nuttig kader voor het ontwerpen van beleid is geschetst, zoals weergegeven in figuur 3. De beleidsontwikkelingscyclus omvat het herkennen van problemen waarvoor een soort beleid moet worden ontwikkeld, het vormen van een beleidsteam, het samenkomen met en verzamelen van de belanghebbenden, het valideren van het beleid, het aannemen van het beleid met elke gewaardeerde resolutie, het afhandelen van het beleid niet na drie jaar, het verminderen van uw beleid, ook het hebben van de feedback en door de verandering. Gedurende het hele proces is het belangrijk om belanghebbenden te betrekken en input te krijgen van verschillende groepen mensen. Het beleid moet ook worden geformaliseerd, om ervoor te zorgen dat het in overeenstemming is met onze organisatiedoelen en eventuele wettelijke vereisten. Beleidsregels moeten regelmatig worden herzien en het beleid moeten worden bijgewerkt wanneer het verouderd is. Er zouden regelmatige evaluaties moeten plaatsvinden en de updates waren noodzakelijk. Beleid zal dienovereenkomstig veranderingen in de omgeving in een organisatie of een bepaalde context uitdagen en ook uitvoeren.(Lubua & Pretorius, 2019)

Figuur 3: Beleidsontwikkelingscyclus



Bron: (Lubua & Pretorius, 2019)

2.2.2. Regelmatige opleiding

Een essentiële overweging bij het opleiden van werknemers over de beste praktijken op het gebied van cyberhygiëne is het onderzoeken van de vele factoren die van invloed zijn op hun gedrag en kennis. In een recente studie van pints blijkt dat gebruikers zich vaak niet bewust zijn van de belangrijkste acties die ze moeten ondernemen en de impact ervan, waardoor hun gedrag wordt beïnvloed. De meeste gebruikers

begrijpen niet wat het precies zou betekenen om de beste beveiligingspraktijken te volgen als ze zich bewust zijn van de risico's. Een aanzienlijk aantal gebruikers kan zich ook bewust zijn van de risico's, maar kan nog steeds niet de juiste voorzorgsmaatregelen nemen om het concept van beveiliging beter te begrijpen. Een andere studie geeft de factoren zoals menselijke factoren die bijdragen aan cyberinbreuken en risico's. Slechte praktijken op het gebied van cyberhygiëne, gebrek aan bewustzijn, gedragsvooroordelen, hiaten in het onderwijs en ontoereikende training dragen aanzienlijk bij aan menselijke factoren die door onderwijs kunnen worden aangepakt en bewustzijn kunnen de kwetsbaarheid in grote mate verminderen en zo ook de cyberweerbaarheid vergroten.(Cain, Edwards, & Still, 2018)(Neigel, Claypoole, Waldfogle, Acharya, & Hancock, 2020)

Cybersecurity-training voor werknemers is essentieel, zodat organisaties proactief een aanpak kunnen volgen om hun informatie te beschermen. Training van werknemers leidt niet alleen werknemers op, maar maakt ook alle werknemers bewust van het soort cyberdreigingen dat er is, wat de gevolgen kunnen zijn van een succesvolle aanval van een cybercrimineel en hoe deze tegen te gaan als deze een organisatie zou destabiliseren. De organisatie moet al haar werknemers opleiden om hen goed geïnformeerd te maken over cyberbeveiliging en om elke bedreiging voor de waardevolle activa van het bedrijf uit te leggen. (Singh, Mohanty, Swagatika, & Kumar, 2020)

Hier zijn enkele best practices voor training op het gebied van cybercyberbeveiliging: (Mughal, 2019)

- Regelmatige training: Blijf beveiligingstraining geven aan eindgebruikers van het bedrijf om hen op de hoogte en up-to-date te houden over de nieuwe bedreigingen die altijd binnen hun verantwoordelijkheden vallen.
- Op maat gemaakte of aangepaste inhoud: Gebruik altijd aangepaste of op maat gemaakte trainingsinhoud die is gebaseerd op het risico van het IoT-apparaat en de rol van de eindgebruiker.
- Interactief leren: Het is belangrijk om te weten wat de eindgebruikers bezighoudt en hun leerproces van de kennis van de rip, het helpt om te interageren en workshops te simuleren om de gebruiker op deze manier te blijven betrekken.
- Duidelijke communicatie: Communiceer altijd het beleid met betrekking tot de IoT-beveiliging en -beperkingen op basis van de beste praktijken en de gebruiker is hiervan op de hoogte.
- Versterking en herinneringen: Blijf de eindgebruiker herinneren aan de beveiliging en blijf altijd zorgen voor het bewustzijn van de eindgebruikers.
- Stimulansen en beloningen: Zorg voor en stimuleer goede praktijken op het gebied van cyberbeveiliging door eindgebruikers te belonen en aan te moedigen de training te volgen of incidenten te melden.
- Evaluatie en feedback: Bewaak het gedrag van de gebruiker en hoe de programmamedewerker werkt als er enige betrokkenheid is getoond.

2.2.3. Organisatiecultuur

Hoe kan het concept van culturele paraatheid worden toegepast op de paraatheid van uw eigen organisatie op het gebied van cyberbeveiliging? Uit onderzoek is gebleken dat organisaties met een sterke cultuur voor cybersecurity beter voorbereid zijn op het omgaan met cyberdreigingen. De cyberbeveiligingscultuur is een

integraal onderdeel van de algehele organisatiecultuur, die vorm geeft aan de kaders voor risicobeheer, governance, beleid en het gedrag van werknemers die verband houden met cyberbeveiliging. Bovendien kunnen organisaties de naleving van het informatiebeveiligingsbeleid door werknemers bevorderen door gebruik te maken van de ondersteuning van het topmanagement en de organisatiecultuur door gebruik te maken van het leiderschap van het topmanagement door te pleiten voor beveiligingsinitiatieven, effectieve communicatie en actieve betrokkenheid van werknemers. Een gemeenschappelijke beveiligingscultuur helpt alle medewerkers, ongeacht hun afdeling of functie, om de risico's van cyberdreigingen te begrijpen. Dit helpt om hun strategieën voor het beperken van die informatiebeveiligingsrisico's beter op elkaar af te stemmen. (Berlilana, Noparumpa, Ruangkanjanases, Hariguna, & Sarmini, 2021) (AL-Nuaimi, 2024) (Hu, Dinev, Hart, & Cooke, 2012) (Fritzvold, 2017)

Het Technology-Organization-Environment (TOE)-framework, dat is ontwikkeld door Tornatzky en Fleischer (1990), is een uitgebreid framework dat een basis biedt voor het onderzoeken van de acceptatie van een verscheidenheid aan producten en diensten op het gebied van informatiesystemen (IS) en informatietechnologie (IT) door organisaties. Dit kader vertegenwoordigt niet alleen het technische aspect van de innovatie, maar ook de organisatorische en ecologische visie om de adoptie van een technologie uit te leggen en te onderzoeken. Het TOE-raamwerk omvat dan ook deze drie dimensies om een duidelijk totaalbeeld te schetsen van de factoren die van invloed zijn op de adoptie van innovaties in organisaties. Volgens de belangrijkste factoren die van invloed zijn op de gereedheid voor cyberbeveiliging in organisaties op basis van het TOE-raamwerk, zijn onder meer: (Gangwar, Date, & Ramaswamy, 2015)(Rahayu & Day, 2015)(Hasan, Ali, Kurnia, & Thurasamy, 2021)

Technologische factoren

De volwassenheid van de IT-infrastructuur van de organisatie speelt een belangrijke rol bij het verbeteren van de paraatheid van een organisatie om cyberaanvallen tegen te gaan. Volwassen zijn in de IT-infrastructuur door over de vereiste middelen te beschikken die zijn experts, IT-apparaten en gebruikerssoftwaretoepassingen waarschuwen, kan leiden tot een betere paraatheid.

Organisatorische factoren

Ondersteuning van het topmanagement op het gebied van cyberbeveiliging, organisatiestructuur en organisatiecultuur zijn belangrijke factoren voor de paraatheid bij cyberaanvallen. De ondersteuning van het topmanagement heeft een positief significant effect op de paraatheid voor cyberbeveiliging.

Milieufactoren

Relaties tussen leveranciers en partners, overheidsvoorschriften en industrieel beleid zijn externe omgevingsfactoren die positief bijdragen aan het vergroten van de paraatheid van de organisatie om cyberaanvallen tegen te gaan

Het ontwikkelen van een cyberbeveiligingscultuur is een complex proces waarbij rekening wordt gehouden met organisatiecultuur, subculturen en kaders. Organisatiecultuur is geïdentificeerd als een essentiële factor bij het vormgeven van beveiligingsculturen en beveiligingscultuur is gedefinieerd als een subcultuur binnen een organisatie. Om een beveiligingscultuur tot stand te brengen die deel uitmaakt van de organisatie, kan de organisatie de cultuur verkennen aan de hand van dimensies zoals artefacten en waarden voorstellen, gedeelde aannames, organisatorische kennis en de vereiste operationele praktijken.(Uchendu, Nurse, Bada, & Furnell, 2021)

Laten we Unit 1 en Unit 2 samenvoegen: dagelijkse gewoonten voor een betere digitale hygiëne

Een robuuste digitale hygiënecultuur is een must in het steeds evoluerende ecosysteem van start-ups. Deze cultuur, gedreven door het management van bovenaf, benadrukt het belang van cyberbeveiliging en gegevensbescherming. Om deze cultuur te bevorderen, moeten start-ups regelmatige back-ups implementeren met hybride bescherming, waarbij gegevens zowel ter plaatse als in de cloud worden opgeslagen. Dit helpt beschermen tegen cyberaanvallen en systeemstoringen en zorgt ervoor dat de gegevens te allen tijde veilig zijn. Versleutelde back-ups zijn ook van het grootste belang, vooral voor sectoren zoals de gezondheidszorg waar naleving van gegevensbescherming niet onderhandelbaar is.

Het is essentieel om antimalwaresoftware in te zetten die een uitgebreide reeks functies biedt, waaronder realtime scannen, gedragsbewaking, e-mailbeveiliging en webfiltering om systemen te beschermen tegen infectie met schadelijke software. Aan de andere kant moeten start-ups regelmatig proactieve cyberbeveiligingsrisicobeoordelingen uitvoeren om mogelijke bedreigingen te bepalen en de waarschijnlijkheid en gevolgen ervan, en de risiconiveaus te evalueren. De beoordelingen zullen als leidraad dienen voor de implementatie van effectieve risicobeperkende maatregelen om kritieke systemen te beschermen.

Het ontwikkelen van uitgebreide beleidsregels en protocollen voor gegevensbeheer om een veilige omgang met gegevens mogelijk te maken, is een prioriteit. Beleid moet beleid en procedures beschrijven voor best practices op het gebied van gegevensbescherming, veilige communicatie en goede digitale hygiëne. Regelmatige training voor medewerkers Het personeel moet beter worden geïnformeerd over de digitale dreigingen en wat ze kunnen doen om deze te helpen voorkomen. Zo blijft uw personeel op de hoogte van de nieuwste dreigingen en beveiligingsmaatregelen.

Open communicatie die werknemers in staat stelt om op een comfortabele manier beveiligingsproblemen aan de orde te stellen, verdachte activiteiten te melden en mogelijke bedreigingen te bespreken, is van vitaal belang voor het beveiligen van de omgeving. Het hebben van een goede dagelijkse cyberhygiëne, zoals het maken van sterke wachtwoorden, het bijhouden van softwarepatches, het versleutelen van gegevens en het gebruik van beveiligde communicatiekanalen, moet een gewoonte worden voor werknemers.

Een ander kosteneffectief element om te overwegen is het kijken naar verschillende anti-malwareoplossingen, de kosten, ondersteuning, updates en compatibiliteit met uw budget en de manier waarop u werkt. Net zoals startups niet zouden moeten overwegen om de bovenstaande elementen als add-ons toe te voegen, zouden startups deze elementen niet als add-ons moeten behandelen. Startups moeten online veilig zijn, hun activa beschermen en vertrouwen opbouwen met hun klanten en partners, dus om dit te doen, moeten startups digitale hygiëne en cyberbeveiliging onderdeel maken van hun DNA. Startups moeten digitaal onderhoud verweven en cyberhygiëne verweven in hun dagelijkse operationele activiteiten, wat de enige echte manier is om de online veiligheid van startups te verhogen en zo cyberweerbaar te maken. Cyberhygiëne is tandenpoetsen en veilige digitale praktijken, terwijl cyberbeveiliging een gebitsbeschermer heeft bovenop het tandenpoetsen. Aanbetaling heb je de ene, je kunt de andere niet hebben, beide zijn zeer vereist.

Unit 3 - Integratie van digitale hygiëne: casestudy en 1 goede praktijk van startups

Best practices: de beste tools voor digitale hygiëne voor startups

Context: In dit digitale tijdperk is het van groot belang dat start-ups en speciale bedrijven sterk afhankelijk zijn van technologie voor hun operationele activiteiten, om de digitale hygiëne te waarborgen om zich te beschermen tegen alle digitale bedreigingen en inbreuken op gegevens. Elke start-up moet over bepaalde digitale hygiënetools beschikken die hen helpen hun digitale activa te beschermen, zodat ze hun operationele activiteiten zonder enige onderbreking kunnen voortzetten.

Het identificeren van de beste digitale hygiënetools: Startups moeten zichzelf uitrusten met een reeks digitale hygiënetools om verschillende aspecten van cyberbeveiliging aan te pakken. Hier is een lijst met enkele tools van bedrijven en organisaties die door grote aantallen mensen worden vertrouwd.

1. **Antivirussoftware**: Antivirussoftware is een controlesysteem dat virussen en andere malware in bepaalde software blokkeert, detecteert en elimineert, en de gegevens beschermt tegen online bedreigingen.

2. **Firewalls**: Een ander netwerkbeveiligingssysteem zijn de firewalls voor internetbeveiligingsapparaten die zijn ontworpen om ongeoorloofde toegang tot een netwerk te voorkomen.
3. **Wachtwoordmanagers**: Deze helpen bij het maken en onderhouden van sterke, unieke wachtwoorden voor alle sites.
4. **Versleutelingstools**: Versleutel gegevens zowel in rust als tijdens het transport en zorg ervoor dat gevoelige gegevens onleesbaar zijn voor onbevoegde gebruikers.
5. **Twee-factor-authenticatie (2FA):** Voegt extra beveiliging toe tijdens een inlogproces.
6. **Virtual Private Networks (VPN):** Biedt veilige en versleutelde verbindingen om de privacy en gegevensbeveiliging via openbare netwerken te behouden.
7. **Veilige cloudopslag**: biedt een plek waar u op een veilige plek een back-up van uw bestanden kunt maken. Door alleen bepaalde mensen toe te laten om erbij te komen.

De effectiviteit van digitale hygiënetools testen

Eerst moeten we ervoor zorgen dat de tools die we hebben gekozen nuttig waren:

1. **Compatibiliteitscontrole**: Zorg ervoor dat de gekozen tools compatibel zijn met de huidige systemen van de startup en bovendien de workflows niet verstoren.
2. **Bruikbaarheidsbeoordeling**: We moeten taken uitvoeren met behulp van de tools. Om succesvol te zijn in het uitvoeren van dagelijkse taken met behulp van de tool, kost het niet te veel tijd en gegevensinvoer
3. **Beveiligingsaudit**: Om de effectiviteit te testen, zullen de tools regelmatig worden uitgevoerd om te zien of ze echt veilig zijn tegen de nieuwste vormen van cyberdreigingen
4. **Training en bewustwording**: Het team voorlichten over het belang van digitale hygiëne en ethisch en correct gebruik van de tools.

Een cultuur van digitale hygiëne tot stand brengen

Context Het creëren van een cultuur van cyberhygiëne in elke startup is net zo belangrijk als de technologie zelf. Bewustzijn en paraatheid voor cyberbeveiliging is het idee om een omgeving te bevorderen waarin elke werknemer in elke start-up het belang van cyberbeveiliging en hun rol bij de bescherming tegen een dreiging erkent.

Het opzetten van een cultuur van digitale hygiëne in uw bedrijf:

1. **Voorbeeld van leiderschap**: Directe leiders moeten het goede voorbeeld geven en een goede digitale hygiëne hebben.
2. **Regelmatige training**: Leid werknemers op als er nieuwe bedreigingen ontstaan.
3. **Duidelijk beleid**: Zorg voor duidelijke en goed gedefinieerde interne beleidsregels voor een goede digitale hygiëne.

4. **Open communicatie aanmoedigen**: Creëer een cultuur waarin werknemers worden beloond voor het kennen of zien van digitale hygiëneproblemen.
5. **Naleving belonen**: Beloon werknemers die laten zien dat ze de basislijn op het gebied van digitale hygiëne overtreffen.

Resultaten en impact Verwachte resultaten van een cultuur van digitale hygiëne voor een Startup:

- **Verminderd risico op cyberaanvallen**: Een goed geïnformeerd team is de eerste verdedigingslinie.
- **Verbeterde gegevensbescherming**: Bescherm uw bedrijven en die van uw klanten met de juiste digitale hygiëne.
- **Naleving van de regelgeving** Volg de cyberbeveiligingsvoorschriften en vermijd financiële en andere boetes.

Belangrijkste conclusies: Start-ups moeten de basis goed krijgen als ze op de lange termijn willen slagen. Het gebruik van de beste digitale hygiënetools en het inbedden van een cyberweerbaarheidscultuur in het bedrijf is essentieel om de langetermijnkosten van een inbreuk te verminderen en de herstelperiode te versnellen als het ergste gebeurt.

Casestudy: SecureTech Startup - Digitale hygiëne omarmen voor cyberbeveiliging

Samenvatting: SecureTech is een fintech-startup die het belang van digitale hygiëne inzag als onderdeel van het beveiligen van hun bedrijf. Deze casestudy geeft een overzicht van de verschillende tools en culturele verschuivingen die ze in hun organisatie hebben doorgevoerd om een nog grotere kloof te creëren voor aanvallers om door te breken in hun digitale ruimte.

Inleiding: In een tijdperk van snelle evolutie van cyberdreigingen heeft SecureTech een zeer zware taak om zijn digitale activa en klantgegevens te beschermen. Tijdens de vroege stadia van de start-up begrijpt het management van het bedrijf het feit dat robuuste digitale hygiëne niet alleen een noodzaak voor hen is, maar ook een zeer cruciaal concurrentievoordeel.

Situatieanalyse: Na een eerste cyberbeveiligingsbeoordeling ontdekte het bedrijf dat er nog veel verbeterpunten zijn. SecureTech heeft de te gebruiken tools op het gebied van digitale hygiëne en het algemene cybersecuritybewustzijn van medewerkers verbeterd.

Identificatie van digitale hygiënetools: Na evaluatie van tal van tools die verband houden met digitale hygiëne, heeft SecureTech een suite geïdentificeerd die hun specifieke situatie zal aanpakken.

1. **BitDefender**: Beschermt al uw apparaten tegen verschillende bedreigingen.
2. **Cisco Firewalls**: Bewaakt en controleert het netwerkverkeer.
3. **LastPass**: wachtwoordmanager bij uitstek.

4. **VeraCrypt**: Versleutelt al uw gegevens.
5. **Duo Security**: Wordt gebruikt voor tweefactorauthenticatie.
6. **NordVPN:** Beschermt uw externe verbinding en werk tegen nieuwsgierige blikken.
7. **Dropbox Business**: slaat je back-ups en bestanden veilig op in de cloud.

Het creëren van een cultuur van digitale hygiëne: Het leiderschap van SecureTech ontwierp en introduceerde een digitaal hygiëneprogramma in het bedrijf.

Betrokkenheid van de CEO: Ondersteuning voor het gebruik van het programma in het hele bedrijf werd geholpen door de CEO die het zijn stempel van goedkeuring gaf.

1. **Maandelijkse cybersecurity-training**: Er werden workshops gehouden om het team op de hoogte te houden van de nieuwste bedreigingen en trends.
2. **Digitaal hygiënehandboek:** Een uitgebreide set beleidsregels en processen werd als Desk Drop aan alle medewerkers verstrekt.
3. **Kampioenen op het gebied van beveiliging:** Geselecteerde medewerkers werden opgeleid tot Cybersecurity Advocates voor hun respectievelijke afdelingen.
4. **Beloning en erkenning voor veilige gewoonten:** Personen met een uitstekende digitale hygiëne werden erkend en beloond.

Uitdagingen en oplossingen: De bezwaren tegen onze verandering: adoptie van nieuwe tools, culturele verschuiving in onze digitale hygiënepraktijken.

1. Vermindering van wegversperringen: Ervoor zorgen dat onze nieuwe digitale toolkits de efficiëntie van elk van onze teams verhoogden in plaats van ze te vertragen.

2. Beveiligingstraining leuk maken: Implementeerde een op games gebaseerd beveiligingstrainingsprogramma dat teams zou rangschikken op basis van hun cybervaardigheden.

3. **Onze troepen op de hoogte houden:** Voortdurend gecommuniceerd over de vooruitgang die TeamSecureTech boekt en de IMPACT die hun inspanningen op het gebied van digitale hygiëne hadden op de beveiliging van hun bedrijf.

Resultaten: Binnen een jaar rapporteerde SecureTech:

• **100% adoptie van digitale hygiënetools –** De gekozen tools werden volledig geadopteerd door het personeel

• **80% vermindering van phishing-pogingen –** Verhoogd bewustzijn van het personeel zorgde voor snellere herkenning en melding van verdachte e-mails

• **Verbeterde nalevingshouding – Er** werd aan alle wettelijke normen voldaan en er werden geen boetes opgelegd

Conclusie: De zeer proactieve houding van SecureTech op het gebied van digitale hygiëne heeft de cyberbeveiliging sterk verbeterd en een cultuur van waakzaamheid en verantwoordelijkheid ontwikkeld. Deze casestudy illustreert hoe een complexe bedreigingsomgeving kan worden verslagen door middel van een effectief controlekader dat samenwerkt met de cultuurtransformatie van een bedrijf.

Conclusies:

Het selecteren van de juiste tool is van groot belang: startups moeten op zoek naar digitale hygiënetools die passen bij hun specifieke behoeften en workflows

Cultuur stimuleert naleving: het opbouwen van een sterke cultuur van digitale hygiëne kan cyberbeveiligingsrisico's verminderen

Het is een proces van verbetering: cyberbeveiliging is geen toestand maar een continu proces, het is geen eenmalige actie en heeft regelmatige updates en trainingen nodig

Verwijzingen

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).

Module 3 - Digitale hygiëne bij startups

Unit 1 - De rol van digitale hygiëne bij de groei en beveiliging van start-ups

Net als het behouden van een goede lichamelijke gezondheid, is het handhaven van robuuste digitale hygiëne de sleutel tot veiliger online zijn. Digitale hygiëne moet voor ons allemaal een routine worden, zowel in ons persoonlijke online leven als in onze professionele activiteiten.

Als start-ups moet u bij het definiëren van interne regels en beleid ook digitale hygiëneregels en best practices opnemen die door alle werknemers moeten worden gevolgd.

De meeste van onze werkzaamheden worden uitgevoerd met behulp van online digitale omgevingen. U moet zich dus bewust zijn van de mogelijke risico's en specifiek beleid implementeren om deze te beperken en een goede digitale hygiëne in uw startup te behouden.

Voordat u overweegt een digitaal hygiënebeleid in te voeren, slechts een formele taak die u moet controleren, moet u nadenken over alle voordelen die het kan opleveren.

Het implementeren van een digitaal hygiënebeleid voor uw startup is dus niet leuk, maar een must-have om het professionele en persoonlijke leven van uw werknemers te beschermen. Als je enkele redenen nodig hebt om de noodzaak van digitale hygiënepraktijken bij startups te benadrukken, laten we dan een paar redenen bekijken waarom digitale hygiëne voor hen cruciaal is.

Startups zijn kleine organisaties, met beperkte middelen en zonder de sterke beveiligingsinfrastructuur van grotere organisaties. Dit maakt ze aantrekkelijke doelwitten voor cybercriminelen en vatbaarder voor cyberdreigingen. Een digitaal hygiënebeleid helpt bij het implementeren van efficiënte beveiligingsmaatregelen en het beperken van mogelijke risico's.

Kortom, voor startups dient een digitaal hygiënebeleid als een fundamenteel element voor beveiliging, het opbouwen van vertrouwen, schaalbaarheid, kosteneffectiviteit en operationele efficiëntie. Het helpt de toon te zetten voor verantwoorde en veilige digitale praktijken, wat cruciaal is voor het aanhoudende succes en de groei van de startup in het digitale bedrijfslandschap van vandaag.

Unit 2 - Voordelen van het implementeren van digitale hygiënepraktijken in startups

Wat zijn de voordelen van het implementeren van goede digitale hygiënepraktijken?

Simpel gezegd, het beoefenen van goede digitale hygiëne maakt uw online aanwezigheid veilig en gezond in het door technologie gedreven zakelijke landschap van vandaag. De voordelen liggen dus op twee niveaus:

1. **Beveiliging en onderhoud**
2. **Gezondheid**

Laten we eens kijken naar de belangrijkste voordelen!

1. **Beveiliging en onderhoud**

Door een goed digitaal hygiënebeleid en best practices te implementeren, blijft uw digitale omgeving op de werkplek (en persoonlijke) veilig. Vergeet niet om onderhoudsregels te definiëren, om er zeker van te zijn dat alle medewerkers op de hoogte zijn van het interne beleid en dat de regels up-to-date zijn met nieuwe mogelijke bedreigingen.

Het is aan te raden om periodieke bewustmakingstrainingen op het gebied van cybersecurity uit te voeren, om er zeker van te zijn dat uw team over de nodige kennis beschikt om goed te reageren op mogelijke nieuwe cyberdreigingen.

Hoe kunnen we de belangrijkste voordelen voor startups samenvatten wanneer ze goede digitale hygiënepraktijken implementeren en handhaven om hun veiligheid in de digitale omgeving te beschermen?

- **Beveiliging en naleving van gegevensprivacy**

De bescherming van gevoelige informatie is cruciaal. Het regelmatig bijwerken van software, het gebruik van sterke wachtwoorden en het implementeren van versleutelingstechnieken kan helpen om gevoelige gegevens te beschermen tegen cyberdreigingen. Goede digitale hygiëne helpt bij het beschermen van gevoelige informatie en voorkomt ongeoorloofde toegang, waardoor het risico op datalekken wordt verkleind. Het naleven van de regelgeving inzake gegevensbescherming zorgt ervoor dat de startup juridische problemen vermijdt en vertrouwen opbouwt bij klanten.

Ook is het beschermen van financiële en klantgegevens van het grootste belang voor startups. Digitale hygiëne zorgt voor veilige online transacties en de integriteit van financiële gegevens.

- **Reputatiemanagement en vertrouwen opbouwen**

Klanten en partners vertrouwen op bedrijven die prioriteit geven aan digitale beveiliging. Door blijk te geven van toewijding aan digitale veiligheid en privacy kan de reputatie van de startup worden verbeterd en vertrouwen worden opgebouwd bij klanten, investeerders en partners. Ook kan de negatieve impact van beveiligingsincidenten worden vermeden. Goed onderhouden digitale assets, waaronder een gebruiksvriendelijke website en veilige online transacties, dragen bij aan een professionele uitstraling.

- **Compliance en juridische bescherming: voldoen aan wettelijke vereisten**

Veel industrieën hebben strikte regels met betrekking tot gegevensbescherming en privacy. Door zich te houden aan branchespecifieke regelgeving en nalevingsnormen kunnen startups juridische complicaties, boetes en reputatieschade voorkomen. Het aannemen van deze regelgeving beschermt de start-up niet alleen tegen juridische gevolgen, maar helpt ook bij het opbouwen van een betrouwbaar merkimago.

Audits en beoordelingen zijn een ander belangrijk aspect. Het regelmatig controleren van digitale praktijken zorgt ervoor dat de startup blijft voldoen aan de veranderende regelgeving en industrienormen.

- **Operationele continuïteit: downtime beperken**

Cybersecurity-incidenten, zoals malware-aanvallen of gegevensverlies, kunnen leiden tot aanzienlijke downtime. Digitale hygiënemaatregelen helpen bij het voorkomen en beperken van dergelijke incidenten en zorgen voor een ononderbroken bedrijfsvoering.

- **Kostenbesparingen: financiële verliezen vermijden**

Herstellen van een cybersecurity-incident kan duur zijn. Regelmatige back-ups en veilige opslagmethoden kunnen gegevensverlies voorkomen, waardoor het opstarten wordt behoed voor de mogelijk hoge kosten die gepaard gaan met het herstellen van verloren informatie. Vroegtijdig investeren in digitale beveiligingsmaatregelen is een proactieve aanpak die mogelijke financiële verliezen als gevolg van cyberaanvallen, zoals ransomware of datalekken, helpt voorkomen.

- **Innovatie en groei: innovatie bevorderen**

Een veilige digitale omgeving stelt startups in staat zich te concentreren op innovatie zonder voortdurend te worden afgeleid door zorgen over cyberbeveiliging. Dit bevordert de creativiteit en versnelt de groei van het bedrijf. Door routinetaken te automatiseren en digitale workflows te optimaliseren, kunnen startups tijd en middelen vrijmaken om zich te concentreren op innovatie en strategische initiatieven. Goede digitale hygiëne zorgt ervoor dat de startup technologisch voorbereid is om nieuwe tools en technologieën toe te passen en concurrerend te blijven op de markt.

- **Vertrouwen en loyaliteit van de klant: bescherming van klantgegevens**

Klanten zijn eerder geneigd om in zee te gaan met bedrijven die prioriteit geven aan de beveiliging van hun persoonlijke informatie. Digitale hygiëne bouwt het vertrouwen en de loyaliteit van de klant op en draagt bij aan langdurige relaties.

- **Beveiliging van de toeleveringsketen: de veiligheid van leveranciers en partners waarborgen**

Goede digitale hygiënepraktijken gaan verder dan de interne systemen van de startup en omvatten veilige communicatie en gegevensuitwisseling met leveranciers en partners, waardoor een veilige end-to-end toeleveringsketen wordt gegarandeerd.

- **Aanpassingsvermogen aan opkomende bedreigingen: bedreigingen voorblijven**

Digitale hygiëne houdt in dat u op de hoogte blijft van de nieuwste cyberbeveiligingsbedreigingen en maatregelen neemt om deze tegen te gaan. Dit aanpassingsvermogen is cruciaal in het steeds evoluerende landschap van cyberdreigingen.

2. **Gezondheid**

We worden overweldigd door de vele digitale technologieën en online platforms waar we overdag onze tijd aan besteden. We mogen de impact die ze kunnen hebben op onze geestelijke gezondheid niet verwaarlozen. Als we tijdens werktijd de bestaande regels van onze organisaties volgen, moeten we ook in ons persoonlijke leven een goede digitale hygiëne implementeren. Voorzichtig zijn met uw schermtijd, overbelichting en overwerk op sociale media vermijden en een wachtwoordbeheerder en tweefactorauthenticatie voor uw accounts gebruiken, brengt u alleen maar veiligheid.

Het implementeren van goede digitale hygiënepraktijken heeft alleen maar voordelen voor de productiviteit en het moreel van de werknemers. Afleiding wordt verminderd en werknemers kunnen productiever zijn wanneer ze niet constant bezig zijn met beveiligingsproblemen. Een veilige digitale omgeving bevordert een positieve werksfeer en verhoogt het moreel.

Als extra voordelen van het implementeren en onderhouden van digitale hygiënepraktijken kunnen we ook noemen:

- **Efficiënte workflow.** Een goede organisatie van digitale activa en bestanden kan werkprocessen stroomlijnen, waardoor werknemers snel informatie kunnen vinden en taken efficiënter kunnen uitvoeren.
- **Samenwerking.** Digitale hygiënepraktijken, zoals het gebruik van samenwerkingstools en cloudopslag, verbeteren het teamwerk door een gecentraliseerd platform te bieden voor communicatie en het delen van bestanden.

- **Eenvoudige aanpassing aan groei en schaalbaarheid**. Door vanaf het begin schaalbare digitale oplossingen te implementeren, kunnen startups groeien zonder noemenswaardige verstoringen of de noodzaak van grote revisies van de digitale infrastructuur.
- **Flexibiliteit.** Het onderhouden van een schone en georganiseerde digitale omgeving biedt de flexibiliteit om zich aan te passen aan **veranderende zakelijke behoeften en markttrends.**
- **Wendbaarheid.** Startups, die bekend staan om hun wendbaarheid, profiteren van efficiënte workflows en samenwerking die mogelijk worden gemaakt door een goed geïmplementeerd beleid.

Kortom, voor startups dient een digitaal hygiënebeleid als een fundamenteel element voor beveiliging, het opbouwen van vertrouwen, schaalbaarheid, kosteneffectiviteit en operationele efficiëntie. Het helpt de toon te zetten voor verantwoorde en veilige digitale praktijken, wat cruciaal is voor het aanhoudende succes en de groei van de startup in het digitale bedrijfslandschap van vandaag.

Unit 3 - Potentiële bedreigingen en gevolgen van het verwaarlozen van digitale hygiëne

In maart 2023 publiceerde het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) een uitgebreid rapport over cyberbeveiligingsdreigingen en -uitdagingen voor 2030 om het bewustzijn van toekomstige bedreigingen en tegenmaatregelen bij zijn lidstaten en belanghebbenden te vergroten (Mattioli et al., 2023). Veel van de geïdentificeerde bedreigingen zijn nu al relevant en zullen de komende jaren urgent blijven. In oktober 2023 publiceerde hetzelfde bureau een rapport over bedreigingen die in juli 2022 en juni 2023 werden gemeld: ENISA Threat Landscape 2023 (Lella, 2023).

Hoewel het publiek en de belanghebbenden van deze rapporten breed zijn, zowel uit de publieke als de private sector, zijn ze bijzonder relevant in de context van startups. Deze laatste zijn bijzonder kwetsbaar voor cyberdreigingen als gevolg van een combinatie van factoren, die vaak verband houden met hun structuur, beperkte middelen en de snel evoluerende aard van de bedrijfsomgeving. Naarmate opkomende bedrijven voor hun activiteiten steeds meer afhankelijk zijn van technologie en online platforms, worden ze vatbaarder voor cyberaanvallen. Zoals eerder opgemerkt, zijn de mogelijke gevolgen van het slachtoffer worden van cyberdreigingen onder meer datalekken, financiële verliezen, reputatieschade en zelfs bedrijfsonderbreking. Start-ups verwerken vaak gevoelige informatie terwijl ze niet over de infrastructuur en middelen beschikken die grotere organisaties hebben, waardoor ze aantrekkelijke doelwitten zijn voor cybercriminelen die kwetsbaarheden willen misbruiken.

De kwetsbaarheid van startups voor cyberdreigingen kan ook aanzienlijke gevolgen hebben voor de economie in het algemeen en verschillende andere openbare structuren. Verschillende manieren waarop kwetsbaarheden van start-ups van invloed kunnen zijn op bredere economische en maatschappelijke aspecten, zijn bijvoorbeeld economische verliezen, banenverlies en werkloosheid, innovatievertraging, verlies van intellectueel eigendom, erosie van het vertrouwen van klanten, verstoringen van de toeleveringsketen, regelgevende en juridische gevolgen, toegenomen overheidsingrijpen en zelfs zorgen over de nationale veiligheid. Daarom moeten startups alle bestaande en potentiële toekomstige bedreigingen erkennen en het bewustzijn vergroten om zichzelf en de samenleving in het algemeen te beschermen.

Een uitgebreid begrip van cyberdreigingen en de implementatie van robuuste beveiligingsmaatregelen zijn absoluut noodzakelijk voor start-ups om risico's te beperken en een veerkrachtige basis te leggen voor succes op de lange termijn in het digitale domein. Om het bewustzijn van de verscheidenheid aan cyberdreigingen te vergroten, zullen we hieronder de dreigingen presenteren die zijn opgenomen in het rapport "ENISA Threat Landscape 2023" (Lella, 2023).

De belangrijkste bedreigingen die in het rapport zijn opgenomen, zijn ransomware, malware, social engineering, bedreigingen tegen gegevens, denial of service, internetbedreigingen, informatiemanipulatie en aanvallen op de toeleveringsketen. We hebben ze kort gedefinieerd en vervolgens de definities uit het rapport "ENISA Threat Landscape 2023" opgenomen.

1. **Ransomware.** Ransomware is een soort kwaadaardige software die is ontworpen om de toegang tot een computersysteem of bestanden te blokkeren totdat er een geldbedrag of losgeld aan de aanvaller is betaald. Het kan bestanden versleutelen, waardoor ze ontoegankelijk worden voor het slachtoffer.
2. **Malware.** Malware, een afkorting van kwaadaardige software, is een term die wordt gebruikt om software of code te beschrijven die is gemaakt met de bedoeling een computersysteem te beschadigen, gegevens te stelen of de normale werking te verstoren. Het omvat verschillende typen, zoals virussen, wormen en Trojaanse paarden.
3. **Sociale engineering.** Social engineering is een methode om individuen te manipuleren om gevoelige informatie vrij te geven of acties uit te voeren die de veiligheid in gevaar kunnen brengen. Technieken omvatten phishing, imitatie en psychologische manipulatie om menselijk gedrag uit te buiten.
4. **Bedreigingen tegen gegevens.** Bedreigingen tegen gegevens omvatten opzettelijke of onopzettelijke acties die de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens in gevaar brengen. Dit omvat datalekken, lekken of ongeoorloofde toegang tot of openbaarmaking van gevoelige informatie.
5. **Denial of Service (DoS).** Denial of Service is een aanval die tot doel heeft de normale werking van een computersysteem, netwerk of service te verstoren of uit te schakelen, waardoor deze tijdelijk of voor onbepaalde tijd niet beschikbaar is voor gebruikers. Distributed Denial of Service (DDoS) houdt in dat meerdere systemen de aanval coördineren.
6. **Internetbedreigingen.** Internetbedreigingen verwijzen naar opzettelijke of onopzettelijke verstoringen van internet of elektronische communicatie, die storingen, black-outs, afsluitingen of censuur veroorzaken. Deze bedreigingen kunnen het gevolg zijn van verschillende factoren, waaronder cyberaanvallen, technische problemen of door de overheid geleide acties.
7. **Manipulatie van informatie.** Informatiemanipulatie omvat opzettelijke, gecoördineerde inspanningen om waarden, procedures en politieke processen negatief te beïnvloeden. Dit kan het verspreiden van verkeerde informatie, nepnieuws of het uitvoeren van activiteiten omvatten die de publieke opinie manipuleren of de normale informatiestromen verstoren.
8. **Aanvallen op de toeleveringsketen.** Supply Chain Attacks richten zich op de relatie tussen organisaties en hun leveranciers. Deze aanvallen omvatten het in gevaar brengen van de beveiliging

van de toeleveringsketen om ongeoorloofde toegang tot of invloed op een doelorganisatie te krijgen. Voorbeelden hiervan zijn het compromitteren van software-updates of hardwarecomponenten.

Belangrijkste bedreigingen gedefinieerd in het rapport "ENISA Threat Landscape 2023"

"Ransomware

Volgens het rapport Threat Landscape for Ransomware Attacks van ENISA wordt ransomware gedefinieerd als een type aanval waarbij bedreigers de controle over de activa van een doelwit overnemen en losgeld eisen in ruil voor de teruggave van de beschikbaarheid van de activa. Deze actie-agnostische definitie is nodig om het veranderende ransomware-dreigingslandschap, de prevalentie van meerdere afpersingstechnieken en de verschillende doelen, anders dan alleen financieel gewin, van de daders te dekken. Ransomware is opnieuw een van de belangrijkste bedreigingen geweest tijdens de rapportageperiode, met verschillende spraakmakende en veel gepubliceerde incidenten.

Schadelijke voorwerpen

Malware, ook wel kwaadaardige code en kwaadaardige logica genoemd, is een overkoepelende term die wordt gebruikt om software of firmware te beschrijven die bedoeld is om een ongeautoriseerd proces uit te voeren dat een negatieve invloed heeft op de vertrouwelijkheid, integriteit of beschikbaarheid van een systeem.

Sociale engineering

Social engineering omvat een breed scala aan activiteiten die proberen menselijke fouten of menselijk gedrag uit te buiten met als doel toegang te krijgen tot informatie of diensten. Het gebruikt verschillende vormen van manipulatie om slachtoffers te verleiden tot het maken van fouten of het overhandigen van gevoelige of geheime informatie. Gebruikers kunnen worden verleid om documenten, bestanden of e-mails te openen, websites te bezoeken of toegang te verlenen tot systemen of diensten. Hoewel het gebruikte kunstaas en de gebruikte trucs misbruik kunnen maken van technologie, vertrouwen ze op een menselijk element om succesvol te zijn. Dit dreigingscanvas bestaat voornamelijk uit de volgende aanvalsvectoren: phishing, spear-phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps en scareware. Hoewel social engineering-technieken vaak worden gebruikt om

eerste toegang te krijgen, kunnen ze ook in latere stadia van een incident of inbreuk worden gebruikt. Bekende voorbeelden zijn Business E-Mail Compromise (BEC), fraude, imitatie, namaak en, meer recentelijk, afpersing.

Bedreigingen tegen gegevens

Een datalek wordt in de AVG gedefinieerd als elke inbreuk op de beveiliging die leidt tot de onopzettelijke of onwettige vernietiging, het verlies, de wijziging of de ongeoorloofde openbaarmaking van of toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (artikel 4.12 AVG). Technisch gezien kunnen bedreigingen tegen data vooral worden geclassificeerd als datalekken of datalekken. Hoewel ze vaak worden gebruikt als uitwisselbare concepten, brengen ze fundamenteel verschillende concepten met zich mee die meestal liggen in de manier waarop ze gebeuren. Een datalek is een opzettelijke cyberaanval door een cybercrimineel met als doel ongeoorloofde toegang te krijgen en gevoelige, vertrouwelijke of beschermde gegevens vrij te geven. Met andere woorden, een datalek is een opzettelijke en krachtige aanval op een systeem of organisatie met de bedoeling gegevens te stelen. Een datalek is een gebeurtenis (bijv. verkeerde configuraties, kwetsbaarheden of menselijke fouten) die kan leiden tot onbedoeld verlies of blootstelling van gevoelige, vertrouwelijke of beschermde gegevens (opzettelijke aanvallen worden ook wel gegevensblootstelling genoemd).

Bedreigingen tegen beschikbaarheid: Denial of Service

Beschikbaarheid is het doelwit van een overvloed aan bedreigingen en aanvallen, waaronder DDoS. DDoS is gericht op de beschikbaarheid van systemen en gegevens en hoewel het geen nieuwe bedreiging is, speelt het een belangrijke rol in het dreigingslandschap voor cyberbeveiliging6 7. Aanvallen vinden plaats wanneer gebruikers van een systeem of dienst geen toegang hebben tot relevante gegevens, diensten of andere bronnen. Dit kan worden bereikt door de dienst en zijn bronnen uit te putten of de componenten van de netwerkinfrastructuur te overbelasten8.

Bedreigingen voor de beschikbaarheid: internetbedreigingen

Bedreigingen voor de beschikbaarheid van internet verwijzen naar opzettelijke of onopzettelijke verstoringen van internet of elektronische communicatie die leiden tot internetstoringen, black-outs, afsluitingen of censuur. Internetverstoringen kunnen het gevolg zijn van door de overheid geleide internetafsluitingen, cyclonen, zware aardbevingen, stroomuitval, kabelonderbrekingen, cyberaanvallen, technische problemen en militaire acties. Deze bedreigingen worden diversifiërend en groeiender, hebben in deze verslagperiode een nieuw record bereikt en hebben enorme monetaire verliezen veroorzaakt voor de nationale economieën.

Manipulatie van informatie

Buitenlandse informatiemanipulatie en -inmenging (FIMI) beschrijft een meestal niet-illegaal gedragspatroon dat waarden, procedures en politieke processen bedreigt of mogelijk negatief kan beïnvloeden. Dergelijke activiteiten zijn manipulatief van aard en worden op een opzettelijke en gecoördineerde manier uitgevoerd. FIMI kan worden uitgevoerd door statelijke of niet-statelijke actoren, met inbegrip van hun volmachten binnen en buiten hun grondgebied, terwijl we in dit rapport de dreiging bestuderen, ongeacht de oorsprong ervan.

Aanvallen op de toeleveringsketen

Een supply chain-aanval richt zich op de relatie tussen organisaties en hun leveranciers. Voor dit ETL-rapport gebruiken we de definitie zoals vermeld in het ENISA Threat Landscape for Supply Chain Attacks10 waarin een aanval wordt geacht een supply chain-component te hebben wanneer deze bestaat uit een combinatie van ten minste twee aanvallen. Om een aanval te classificeren als een supply chain-aanval, moeten zowel de leverancier als de klant het doelwit zijn. SolarWinds was een van de eerste onthullingen van dit soort aanvallen en toonde de potentiële impact van aanvallen op de toeleveringsketen. Er werd opgemerkt dat bedreigingsactoren zich blijven voeden met deze bron om hun operaties uit te voeren en voet aan de grond te krijgen binnen organisaties, om te profiteren van de wijdverbreide impact en het grote slachtofferbestand van dergelijke aanvallen."

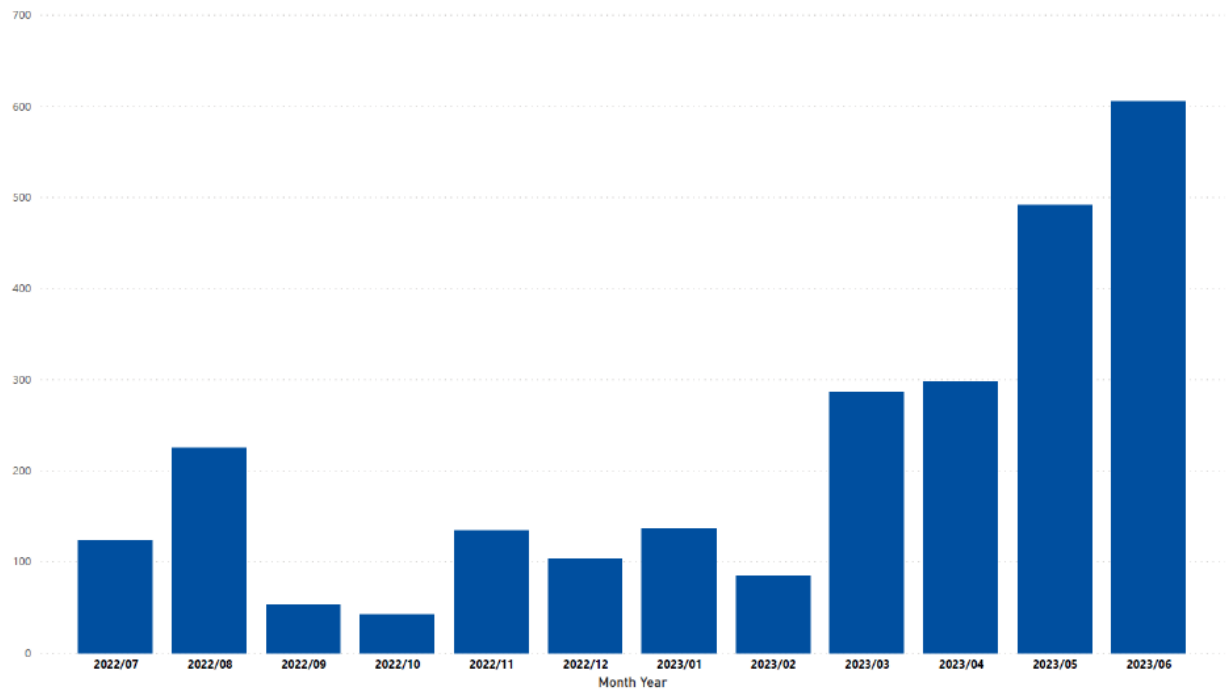
Lella, I.; Tsekmezoglou, E.; Theocharidou, M.; Magonara, E.; Malatras, A.; Naydenov, R.S.; Ciobanu, C. (2023). Enisa-dreigingslandschap 2023. ENISA, blz. 6-8

Naast de hierboven gedefinieerde cyberdreigingen (ransomware, malware, social engineering, bedreigingen tegen gegevens, denial of service, internetbedreigingen, informatiemanipulatie en aanvallen op de toeleveringsketen), kunnen startups te maken krijgen met verschillende andere cyberbeveiligingsbedreigingen. Enkele extra bedreigingen waar u rekening mee moet houden zijn:

1. **Phishing-aanvallen.** Phishing omvat het gebruik van misleidende e-mails, berichten of websites om personen te misleiden om gevoelige informatie vrij te geven, zoals gebruikersnamen, wachtwoorden of financiële gegevens. Phishing-aanvallen kunnen zeer gericht zijn (spear-phishing) of meer wijdverbreid.
2. **Man-in-the-Middle (MitM) aanvallen.** Bij MitM-aanvallen onderschept een ongeautoriseerde entiteit de communicatie tussen twee partijen en wijzigt deze mogelijk. Dit kan leiden tot gegevensdiefstal, afluisteren of injectie van kwaadaardige inhoud in de communicatiestroom.
3. **Zero-day exploits.** Zero-day kwetsbaarheden zijn kwetsbaarheden in software die onbekend zijn bij de leverancier en niet zijn gepatcht. Bedreigingsactoren kunnen deze kwetsbaarheden misbruiken voordat een oplossing is ontwikkeld, wat een risico vormt voor elke organisatie die de getroffen software gebruikt.
4. **Geavanceerde persistente bedreigingen (APT's).** APT's zijn geavanceerde en gerichte cyberaanvallen die doorgaans worden georkestreerd door goed gefinancierde en georganiseerde bedreigingsactoren. Deze aanvallen omvatten vaak een langdurige en sluipende infiltratie van een netwerk, met als doel gevoelige informatie te stelen.
5. **IoT (Internet of Things) kwetsbaarheden.** Naarmate startups steeds meer IoT-apparaten in hun activiteiten integreren, kunnen deze apparaten potentiële doelwitten worden voor cyberaanvallen. Onveilige IoT-apparaten kunnen worden misbruikt om ongeoorloofde toegang tot netwerken te krijgen of aanvallen uit te voeren.
6. **Cryptojacking.** Cryptojacking omvat het ongeoorloofd gebruik van de bronnen van een computer of netwerk om cryptocurrency te minen. Cybercriminelen kunnen systemen infecteren met malware die stilletjes cryptocurrency mint, wat gevolgen heeft voor de systeemprestaties.
7. **Cross-site scripting (XSS).** XSS-aanvallen omvatten het injecteren van kwaadaardige scripts in webpagina's die door andere gebruikers worden bekeken. Dit kan leiden tot diefstal van gebruikersgegevens, sessiekaping of de verspreiding van malware naar andere gebruikers.
8. **SQL-injectie.** SQL-injectieaanvallen vinden plaats wanneer kwaadaardige SQL-code in invoervelden wordt geïnjecteerd, waardoor aanvallers een database kunnen manipuleren. Dit kan leiden tot ongeoorloofde toegang, gegevensmanipulatie of gegevensextractie.

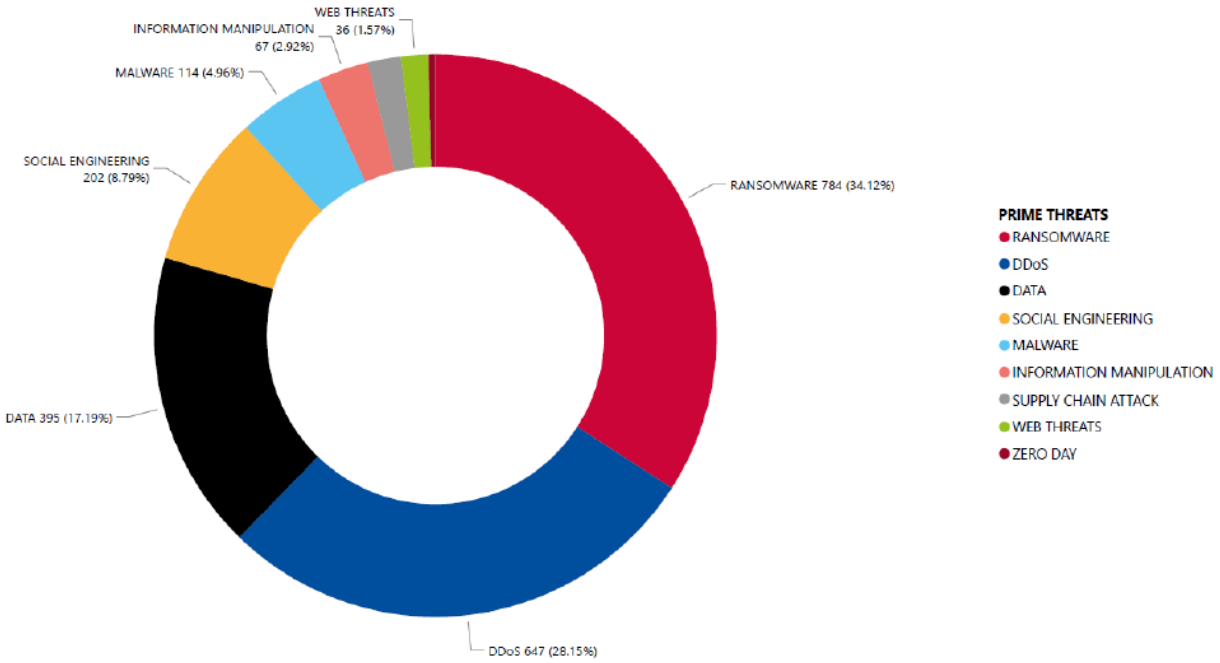
9. **Bestandsloze malware.** Bestandsloze malware werkt in het geheugen in plaats van te vertrouwen op uitvoerbare bestanden. Dit maakt het voor traditionele antivirusoplossingen moeilijker om te detecteren, omdat er mogelijk geen fysiek bestand is om te analyseren.
10. **Credential vulling.** Bij credential stuffing-aanvallen gebruiken cybercriminelen gestolen gebruikersnaam- en wachtwoordcombinaties van de ene service om ongeoorloofde toegang te krijgen tot een andere service waar gebruikers inloggegevens hebben hergebruikt.
11. **DNS-spoofing en cachevergiftiging.** DNS-spoofing omvat het omleiden van DNS-query's (Domain Name System) naar kwaadaardige sites. Cachevergiftiging manipuleert DNS-cachegegevens, waardoor gebruikers naar onbedoelde en mogelijk schadelijke bestemmingen worden geleid.

Zoals gezegd blijkt uit het rapport "ENISA Threat Landscape 2023" (Lella, 2023) dat de belangrijkste bedreigingen wereldwijd en in de EU zijn: ransomware, malware, social engineering, bedreigingen tegen gegevens, denial of service, internetbedreigingen, informatiemanipulatie en aanvallen op de toeleveringsketen.



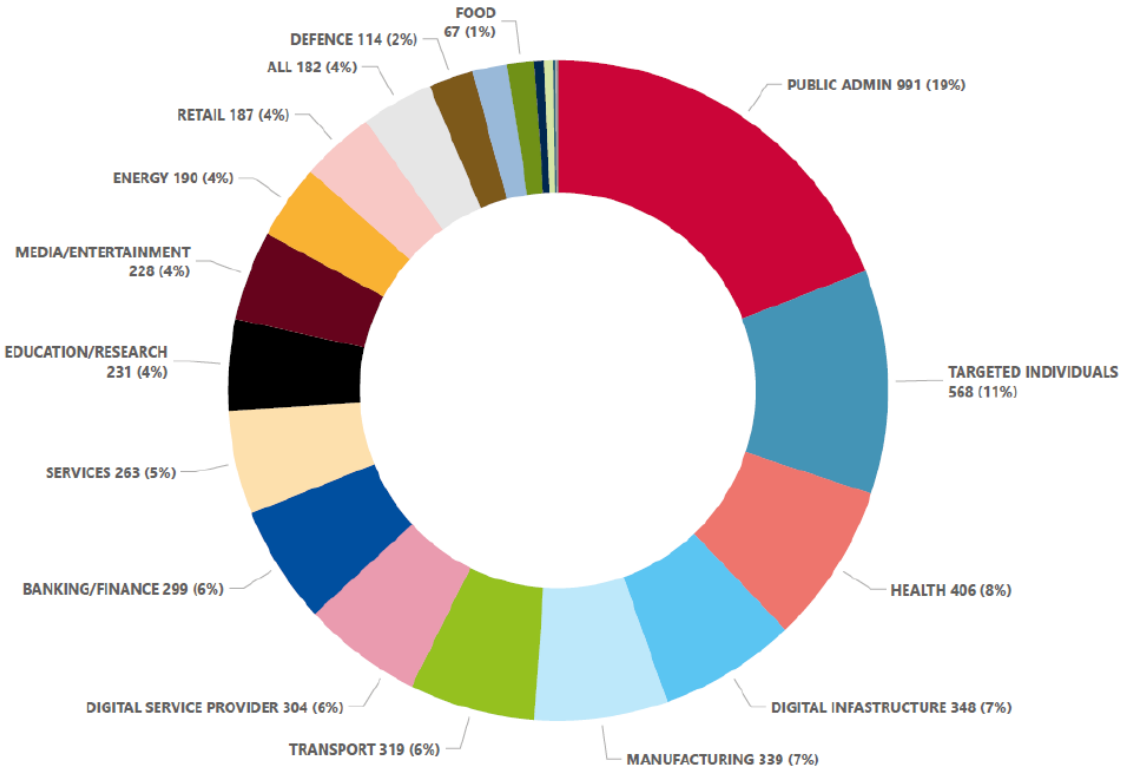
Figuur 1. Tijdlijn van EU-evenementen (telling van het aantal waargenomen incidenten per maand) (Lella, 2023)

Het rapport illustreert (figuur 1) de toename van cyberaanvallen in de eerste helft van 2023. Deze stijging komt zowel op mondiaal als op EU-niveau tot uiting. De toename weerspiegelt misschien niet alleen de toename van het aantal, maar ook het bewustzijn van dergelijke evenementen. Toch is de trend zorgwekkend.



Figuur 2. EU-uitsplitsing van het aantal dreigingen per dreigingsgroep (Lella, 2023)

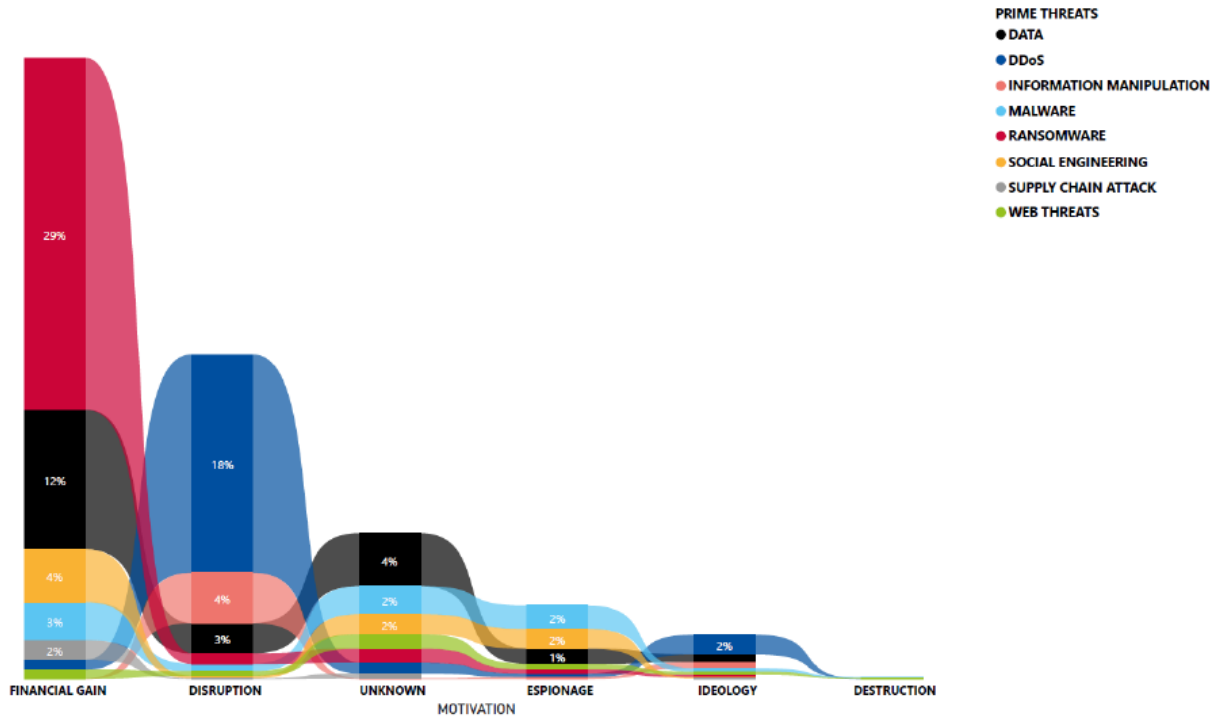
We kunnen in figuur 2 zien dat de meest voorkomende bedreigingen waren: Ransomware, Denial of Service, Bedreigingen tegen data, Social Engineering en Malware. Deze werden gevolgd door informatiemanipulatie, aanvallen op de toeleveringsketen, internetbedreigingen en Zero Day.



Figuur 3. Gerichte sectoren per aantal incidenten (juli 2022 - juni 2023) (Lella, 2023)

Uit een sectorale analyse blijkt dat bedreigingen de grenzen van specifieke industrieën of sectoren overstijgen en hun invloed uitoefenen op een breed spectrum van gebieden (Lella, 2023). Dit kan te wijten zijn aan de hoge interconnectiviteit van de digitale wereld van vandaag.

In het wereldwijde landschap was een groot aantal evenementen gericht op organisaties in het openbaar bestuur (19%) en de gezondheidssector (8%). We kunnen zien dat een van de belangrijkste bedreigde actoren individuen zijn (11%). Hoewel dit misschien geen verband lijkt te houden met startups en de particuliere sector, kunnen deze personen werknemers zijn in sommige startende bedrijven en kunnen ze de bedrijven onbedoeld in gevaar brengen.



Figuur 4. Motivatie van dreigingsactoren per dreigingscategorie (Lella, 2023)

Het rapport presenteert ook de motivaties achter de cyberaanvallen tijdens de gestelde periode (Lella, 2023). Zoals te zien is in figuur 4, hadden de meeste aanvallen financieel gewin, gevolgd door ontwrichting, onbekend, spionage en ideologie. Ransomware is goed voor bijna 30% van de aanvallen die worden uitgevoerd voor financieel gewin, gevolgd door bedreigingen tegen gegevens, social engineering en malware.

Bewust zijn van de redenen achter cyberdreigingen en de soorten bedreigingen kan de strategie die startups gebruiken om digitale hygiënepraktijken te ontwikkelen en te implementeren, informeren en sturen. Startups en de particuliere sector zijn bijvoorbeeld vooral gericht op financieel gewin. Wetende dat ransomware, bedreigingen tegen gegevens, social engineering en malware voornamelijk voor dergelijke doeleinden werden gebruikt, zouden start-ups hun digitale hygiënestrategie kunnen richten op het beschermen van de toegang tot gegevens en het opleiden van klanten en werknemers om zichzelf te beschermen tegen social engineering-bedreigingen.

Om te helpen begrijpen hoe een startup cyberdreigingen moet aanpakken en wat ze moeten doen om zichzelf te beschermen, hebben we een voorbeeld van goede praktijken opgesteld. Dit zal illustreren hoe een bedrijf moet omgaan met mogelijke bedreigingen en hoe het zich moet voorbereiden om cybergebeurtenissen te voorkomen.

Unit 4 – 1 good practice van startups

Om beter te begrijpen hoe bedreigingen kunnen worden geïdentificeerd en hoe u de situatie vooraf kunt aanpakken, laten we het volgende voorbeeld bekijken. We hebben het voorbeeld gericht op de kwetsbaarheid die kan ontstaan door online betalen, een wijdverbreide en veel voorkomende situatie die zowel het bedrijf als de klanten kan treffen in het geval van een cyberaanval.

Digitale hygiëne in de beveiliging van online betalingen

Context

In het snel evoluerende landschap van de ontwikkeling van mobiele apps, waar innovatie kruist met financiële transacties, wordt het waarborgen van de veiligheid van een app die online betalingen verwerkt van het grootste belang. Een voorbeeld is er een van een bedrijf dat een abonnement op een mobiele app aanbiedt, wat een kwetsbaarheid kan veroorzaken in verband met hun betalingsverwerking. De potentiële kwetsbaarheid in hun online betalingsverwerkingssysteem kan zowel het bedrijf als zijn klanten blootstellen aan risico's van financiële fraude.

De startup moet de situatie analyseren, de risico's identificeren en oplossingen implementeren om kwetsbaarheden en financiële fraudesituaties te voorkomen.

Stap 1. De analyse van de situatie

Als eerste stap in het digitale hygiëneproces hebben we de situatieanalyse. Tijdens deze fase is het belangrijk om de kwetsbaarheden te identificeren en het risico en de implicaties van deze kwetsbaarheden in het geval van een inbreuk op de beveiliging te beoordelen.

Identificatie van het beveiligingslek in de betaling:

Het bedrijf voerde een grondige analyse uit van de betalingsverwerkingsfunctionaliteit van de app om potentiële zwakke punten te identificeren, waaronder onveilige betalingsgateways, kwetsbaarheden in transactieversleuteling en mogelijke punten van ongeoorloofde toegang.

Het uitvoeren van een uitgebreide analyse van een betaalapp om mogelijke zwakke punten te identificeren, omvat een systematisch en grondig onderzoek van verschillende componenten binnen de applicatie. Een algemene richtlijn voor het uitvoeren van een dergelijke analyse zou kunnen zijn:

1. **Risicobeoordeling:** Identificeer en begrijp de kritieke componenten van de betalingsapp, waaronder gebruikersauthenticatie, gegevensopslag, betalingsverwerking en communicatie met externe servers.
2. **Controle op naleving van regelgeving:** Zorg ervoor dat de betalingsapp voldoet aan de relevante regelgevingsnormen en nalevingsvereisten in de branche, zoals de Payment Card Industry Data Security Standard (PCI DSS).
3. **Data Flow Mapping:** Breng de stroom van gevoelige gegevens (bijv. creditcardgegevens) binnen de app in kaart, van invoer tot opslag en verzending. Identificeer potentiële kwetsbaarheden in deze gegevensstroom.
4. **Netwerkbeveiliging:** Beoordeel de beveiliging van netwerkcommunicatie, inclusief het gebruik van beveiligde protocollen (HTTPS), versleuteling en SSL-certificaten (Secure Sockets Layer).
5. **Verificatiemechanismen:** Evalueer de sterkte van gebruikersverificatiemechanismen. Implementeer multi-factor authenticatie om een extra beveiligingslaag toe te voegen.
6. **Beveiliging van betalingsgateways:** Onderzoek de integratie met betalingsgateways en zorg ervoor dat veilige en gerenommeerde services worden gebruikt. Werk de betalingsgatewaysoftware regelmatig bij en patch.
7. **Gegevensversleuteling:** Implementeer end-to-end-versleuteling om gevoelige gebruikersgegevens gedurende het hele transactieproces te beschermen.
8. **Scannen op kwetsbaarheden en penetratietests:** Voer regelmatig kwetsbaarheidsscans en penetratietests uit om potentiële zwakke punten te identificeren en echte aanvalsscenario's te simuleren. Dit kan het gebruik van geautomatiseerde tools inhouden of het inhuren van externe beveiligingsbedrijven met expertise op het gebied van penetratietesten.
9. **Code Review:** Voer een grondige codebeoordeling uit om eventuele kwetsbaarheden of zwakke punten in de broncode van de app te identificeren. Zorg ervoor dat coderingspraktijken voldoen aan de best practices op het gebied van beveiliging.
10. **Incidentresponsplan:** Ontwikkel en implementeer een incidentresponsplan om potentiële inbreuken op de beveiliging snel aan te pakken en te beperken. Dit omvat procedures voor het informeren van gebruikers in geval van een beveiligingsincident.
11. **Beveiligingsaudits door derden:** Overweeg om externe beveiligingsbedrijven in te schakelen die gespecialiseerd zijn in beveiligingsaudits van applicaties. Deze bedrijven kunnen een onafhankelijk perspectief en gespecialiseerde expertise inbrengen om kwetsbaarheden te identificeren.

U kunt deze punten gebruiken als een checklist om uw analyse uit te voeren.

Beveiliging is een continu proces en regelmatige beoordelingen en updates zijn cruciaal om opkomende bedreigingen voor te blijven. De punten op de hierboven genoemde checklist kunnen in de loop van de tijd veranderen, afhankelijk van de mogelijke dreigingen en het cyberbeveiligingslandschap. Samenwerken met externe beveiligingsbedrijven of consultants kan aanvullende expertise en inzichten opleveren, vooral als het gaat om grondige beveiligingsaudits en penetratietests. Het is essentieel om prioriteit te geven aan de beveiliging van betalingsapps om zowel het bedrijf als zijn gebruikers te beschermen tegen mogelijke risico's en inbreuken.

Laten we aannemen dat het opstartende beveiligingsteam tijdens een routinematige beveiligingsaudit een mogelijke zwakte identificeert in het coderingsprotocol dat wordt gebruikt voor het verzenden van betalingsgegevens binnen hun mobiele app. Vervolgens moet het team de kwetsbaarheid en de implicaties ervan voor het bedrijf en de gebruikers beoordelen.

Beoordeling van risico's en implicaties:

Na het identificeren van de kwetsbaarheden in de betalingsbeveiliging, is het belangrijk om rekening te houden met risico's en implicaties voor zowel het bedrijf als de gebruikers. Dit deel van het proces omvat het evalueren van de risico's voor het bedrijf en de gebruikers, en het prioriteren van de geïdentificeerde kwetsbaarheden op basis van de potentiële impact.

1. **Effectbeoordeling:** Evalueer de mogelijke impact van een inbreuk op de beveiliging op zowel het bedrijf als zijn gebruikers, rekening houdend met financiële verliezen, reputatieschade en mogelijke juridische gevolgen.
2. **Prioritering:** Prioriteer kwetsbaarheden op basis van de ernst van de potentiële impact en de kans op misbruik.

Tijdens de evaluatie van de risico's die verband houden met de zwakte in het versleutelingsprotocol, evalueert het beveiligingsteam de omvang van de kwetsbaarheid, rekening houdend met factoren zoals het type versleutelingsalgoritme dat wordt gebruikt, de omvang van mogelijke uitbuiting en de impact op de beveiliging van gebruikersgegevens.

De risicoanalyse is bedoeld om inzicht te krijgen in de mogelijke gevolgen van de versleutelingskwetsbaarheid, waaronder het risico van ongeoorloofde toegang tot gevoelige betalingsinformatie en de mogelijke impact op de reputatie van het bedrijf.

Stap 2. Een oplossing vinden

De oplossingen voor mogelijke kwetsbaarheden in de betalingsbeveiliging zijn onder meer:

1. **Veilige integratie van betalingsgateway:** Upgrade het betalingsverwerkingssysteem om te integreren met een veilige betalingsgateway, zodat alle transacties worden versleuteld en beschermd tegen onderschepping tijdens de verzending.
2. **End-to-end encryptie:** Implementeer end-to-end encryptie voor alle betalingstransacties, waardoor gevoelige gebruikersgegevens worden beschermd tegen ongeoorloofde toegang in elke fase van het transactieproces.
3. **Verbeteringen in gebruikersverificatie:** Versterk de maatregelen voor gebruikersverificatie en integreer multi-factor authenticatie om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot de app en transacties kunnen uitvoeren binnen de app.
4. **Regelmatige beveiligingsaudits en nalevingscontroles:** Stel routinematige beveiligingsaudits in die specifiek gericht zijn op de betalingsverwerkingsfunctionaliteit en voert nalevingscontroles uit met industrienormen en -voorschriften.

In de meer specifieke zorg voor de zwakte in het versleutelingsprotocol die we als voorbeeld hebben gebruikt, zou de reactie en mitigatie het volgende omvatten:

1. **Onmiddellijke inperking:** Het bedrijf onderneemt onmiddellijk actie om de kwetsbaarheid in te dammen door het getroffen versleutelingsprotocol tijdelijk uit te schakelen om verdere mogelijke uitbuiting te voorkomen.
2. **Communicatie met belanghebbenden:** Het bedrijf initieert transparante communicatie met zijn gebruikers en informeert hen over de geïdentificeerde coderingskwetsbaarheid, de tijdelijke opschorting van de getroffen functie en de voortdurende inspanningen om het probleem aan te pakken.
3. **Betrokkenheid van beveiligingsexperts:** Het bedrijf maakt gebruik van de diensten van externe cyberbeveiligingsexperts om een diepgaande analyse van de versleutelingskwetsbaarheid uit te voeren en aanbevelingen te doen voor een robuustere en veiligere versleutelingsoplossing.
4. **Ontwikkeling van een patch:** Op basis van de aanbevelingen van de beveiligingsexperts maakt het ontwikkelingsteam een patch die de versleutelingskwetsbaarheid verhelpt. Dit omvat het implementeren van een veiliger coderingsalgoritme en het waarborgen van compatibiliteit met bestaande systemen.
5. **Interne tests:** Voordat de patch wordt geïmplementeerd, voert het bedrijf grondige interne tests uit om ervoor te zorgen dat de bijgewerkte coderingsmaatregelen geen nieuwe kwetsbaarheden introduceren of de functionaliteit van de betalingsapp verstoren.
6. **Implementatie van de patch:** Zodra de patch effectief en veilig wordt geacht, implementeert het bedrijf de update op de apparaten van alle gebruikers, waarbij de betalingsfunctionaliteit wordt hersteld met verbeterde coderingsmaatregelen.

7. **Monitoring na implementatie:** Het bedrijf houdt de prestaties van de app na de implementatie nauwlettend in de gaten om ervoor te zorgen dat de versleutelingspatch de kwetsbaarheid met succes verzacht en geen onvoorziene problemen introduceert.
8. **Gebruikerseducatie:** Om het vertrouwen van gebruikers te herstellen, zou het bedrijf een educatieve campagne binnen de app kunnen lanceren, waarbij gebruikers worden geïnformeerd over de versleutelingskwetsbaarheid en de stappen die zijn genomen om deze aan te pakken, en tips worden gegeven over het handhaven van veilige gebruikspraktijken.

De stappen in deze reactie zijn specifiek voor het geïdentificeerde probleem. Als de beveiligingsaudit een ander probleem identificeert, worden specifieke antwoorden voor dat probleem ingezet.

Stap 3. Resultaten en impact

De gerichte aanpak van het bedrijf voor digitale hygiëne in app-beveiliging voor online betalingen leverde positieve resultaten op:

- Geen gevallen van ongeoorloofde transacties of inbreuken op de beveiliging gedurende een jaar.
- Verhoogd gebruikersvertrouwen en vertrouwen in de app, wat leidt tot een toename van het aantal transacties en positieve gebruikersrecensies.
- Naleving van de branchevoorschriften, waardoor het bedrijf wordt gepositioneerd als een veilig en betrouwbaar platform voor online betalingen.

Kernpunten

Start-ups die apps voor betalingsverwerking aanbieden, kunnen waardevolle inzichten uit dit voorbeeld halen:

- Geef prioriteit aan de integratie van veilige betalingsgateways om transactiegegevens te beschermen.
- Implementeer end-to-end-versleuteling om gebruikersgegevens tijdens het betalingsproces te beschermen.
- Verbeter de maatregelen voor gebruikersauthenticatie en integreer multi-factor authenticatie voor extra beveiliging.
- Voer regelmatig beveiligingsaudits en nalevingscontroles uit om mogelijke kwetsbaarheden voor te blijven en zorg voor afstemming op de industriestandaarden.

Door deze digitale hygiënepraktijken toe te passen, kunnen ontwikkelaars van betalingsverwerkingsapps bijdragen aan het creëren van een veilig en betrouwbaar platform, waardoor het vertrouwen wordt bevorderd van gebruikers die zich bezighouden met online financiële transacties.

Verwijzingen:

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