Startup'lar için El Kitabı

29 ŞUBAT 2024

Co-funded by the European Union

GOOD START

Good Digital Hygiene for Startups

Proje No: 2022-1-LV01-KA220-VET-000086725 | Proje başlığı: Startuplar için İyi Dijital Hijyen

İçindekiler

Modül 1 - Dijital Hijyen Tanımlarını ve Kavramlarını Anlamak

Ünite 1 - Dijital Hijyenin Kavramsal Çerçevesi

Dijital girişimciliğin hızla gelişen ortamında, startup'lar şiddetli rekabetten kaynak kısıtlamalarına kadar sayısız zorlukla karşılaşıyor. Bu zorlukların ortasında, sağlam dijital hijyen uygulamalarının sağlanması, girişimlerin sürdürülebilir büyümesi ve başarısı için çok önemlidir.

Dijital hijyen kavramı, siber güvenlik, bilgi yönetimi ve örgütsel davranış dahil olmak üzere çeşitli alanlardan çeşitli teorik çerçevelere ve ilkelere dayanmaktadır. Dijital hijyen kavramının dayandığı bazı temel teoriler vardır:

1. Siber güvenlik teorisi

Siber güvenlik teorisi, siber tehditleri ve güvenlik açıklarını anlamayı ve ele almayı amaçlayan çeşitli ilkeleri ve modelleri kapsar. CIA Üçlüsü (Gizlilik, Bütünlük, Kullanılabilirlik) siber güvenlik teorisinde temel bir kavramdır ve verilerin yetkisiz erişime karşı korunmasının (gizlilik), veri doğruluğu ve güvenilirliğinin sağlanmasının (bütünlük) ve yetkili kullanıcılar için veri erişilebilirliğinin sürdürülmesinin (kullanılabilirlik) önemini vurgular. Derinlemesine Savunma modeli ve Sıfır Güven modeli gibi diğer siber güvenlik teorileri, riskleri azaltmak ve siber saldırılara karşı savunmak için sağlam siber güvenlik stratejileri tasarlamak ve uygulamak için çerçeveler sağlar.

2. Bilgi yönetimi teorisi

Bilgi yönetimi teorisi, kuruluşlardaki bilgi varlıklarının etkin yönetimine odaklanır. Bilgi yaşam döngüsü yönetimi modeli, bilginin oluşturulmasından elden çıkarılmasına kadar geçtiği aşamaları tanımlayan ve gizlilik, bütünlük ve kullanılabilirliği sağlamak için yaşam döngüsü boyunca bilgiyi yönetmenin önemini vurgulayan teorik bir çerçevedir. Veri yönetişimi, veri yönetimi ve veri kalitesi yönetimi ilkeleri de bilgi yönetimi teorisinin merkezinde yer alır ve kuruluşların veri varlıklarını etkili bir şekilde nasıl yönetebilecekleri ve koruyabilecekleri konusunda yol gösterir.

3. İnsan faktörleri teorisi

İnsan faktörleri teorisi, siber güvenlik bağlamında insan davranışının, bilişinin ve karar vermenin rolünü araştırır. İnsan Hatası Teorisi, insan hatasının siber güvenlik olaylarına ve veri ihlallerine önemli ölçüde katkıda bulunduğunu öne sürmekte ve insanla ilgili risklerin azaltılmasında eğitim, farkındalık ve

kullanılabilirliğin önemini vurgulamaktadır. Planlı Davranış Teorisi ve Teknoloji Kabul Modeli (TAM) bireylerin tutum, inanç ve algılarının siber güvenlik uygulamaları ve teknolojilerini benimsemeye yönelik davranışlarını nasıl etkilediğini açıklayan diğer teorik çerçevelerdir.

4. Örgütsel davranış teorisi

Örgütsel davranış teorisi, örgütler içindeki bireylerin, grupların ve yapıların nasıl etkileşime girdiğini ve davranışı nasıl etkilediğini inceler. Teknoloji-örgüt-çevre çerçevesi, teknolojik faktörler, örgütsel faktörler ve çevresel faktörler de dahil olmak üzere, kuruluşlarda bilgi teknolojilerinin benimsenmesini ve uygulanmasını etkileyen faktörleri açıklayan teorik bir modeldir. Everett Rogers tarafından geliştirilen yeniliklerin yayılması teorisi, yeni fikirlerin, teknolojilerin ve uygulamaların toplumlar ve kuruluşlar içinde nasıl yayıldığını araştırır ve dijital hijyen uygulamalarının girişimler ve diğer kurumsal bağlamlarda benimsenmesi ve yayılmasına ilişkin içgörüler sağlar.

5. Uyumluluk teorisi

Uyum teorisi, bireylerin ve kuruluşların kurallara, düzenlemelere ve normlara uyumunu etkileyen faktörleri ele almaktadır. Planlı davranış teorisi ve gerekçeli eylem teorisi, bireylerin tutumlarına, öznel normlarına ve algılanan davranışsal kontrollerine dayalı olarak kurallara ve düzenlemelere uyma niyetlerini açıklayan teorik modellerdir. Bu teoriler, girişimlerin ve kuruluşların eğitim, öğretim, teşvikler ve yaptırım mekanizmaları yoluyla siber güvenlik yönetmeliklerine ve standartlarına uyumu nasıl teşvik edebilecekleri konusunda fikir vermektedir.

Dolayısıyla, dijital hijyen kavramı, siber güvenlik, bilgi yönetimi, insan davranışı ve startup'lar ve diğer kuruluşlardaki örgütsel dinamiklerin karmaşık zorluklarını ele almak için multidisipliner perspektifleri ve yaklaşımları entegre etmektedir.

Ayrıca ek kavramlar, girişimlerde dijital hijyen uygulamalarının anlaşılması ve uygulanması için bir temel sağlayarak dijital altyapılarının ve operasyonlarının korunmasını, bütünlüğünü ve esnekliğini sağlar:

A) Siber Güvenlik

Siber güvenlik, dijital sistemleri, ağları ve verileri yetkisiz erişimden, siber saldırılardan ve veri ihlallerinden koruma uygulamasıdır. Dijital varlıkları korumayı ve bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamayı amaçlayan çeşitli teknolojileri, süreçleri ve uygulamaları kapsar.

B) Veri Gizliliği

Veri gizliliği, kişisel ve hassas bilgilerin yetkisiz erişim, kullanım veya ifşaya karşı korunması anlamına gelir. Bireylerin gizlilik haklarını korumak için GDPR, HIPAA veya CCPA gibi verilerin toplanması, depolanması ve işlenmesini düzenleyen yönetmeliklere ve standartlara uyulmasını içerir.

C) Risk yönetimi

Risk yönetimi, dijital bir ortamda faaliyet göstermeyle ilişkili risklerin belirlenmesini, değerlendirilmesini ve azaltılmasını içerir. Bir girişimin faaliyetlerini, itibarını veya finansal istikrarını etkileyebilecek potansiyel tehditleri ve güvenlik açıklarını önlemek, tespit etmek ve bunlara yanıt vermek için kontrollerin ve önlemlerin uygulanmasını içerir.

D) Uyum ve düzenleyici çerçeveler

Yasal ve etik operasyonları sağlamak için yönetmeliklere ve endüstri standartlarına uyum, startup'lar için çok önemlidir. GDPR, HIPAA, PCI DSS veya SOX gibi düzenleyici çerçeveler, girişimlerin yasal ve mali yansımalardan kaçınmak için uyması gereken veri koruma, güvenlik ve gizlilik için yönergeler ve gereksinimler sağlar.

E) Bilgi güvenliği yönetim sistemleri (BGYS)

ISO/IEC 27001 gibi BGYS çerçeveleri, kuruluşlardaki bilgi varlıklarını yönetmek ve korumak için sistematik bir yaklaşım sağlar. Riskleri yönetmek, uyumluluğu sağlamak ve bilgi güvenliği uygulamalarını sürekli iyileştirmek için politikalar, prosedürler ve kontroller içerirler.

F) Veri yönetişimi

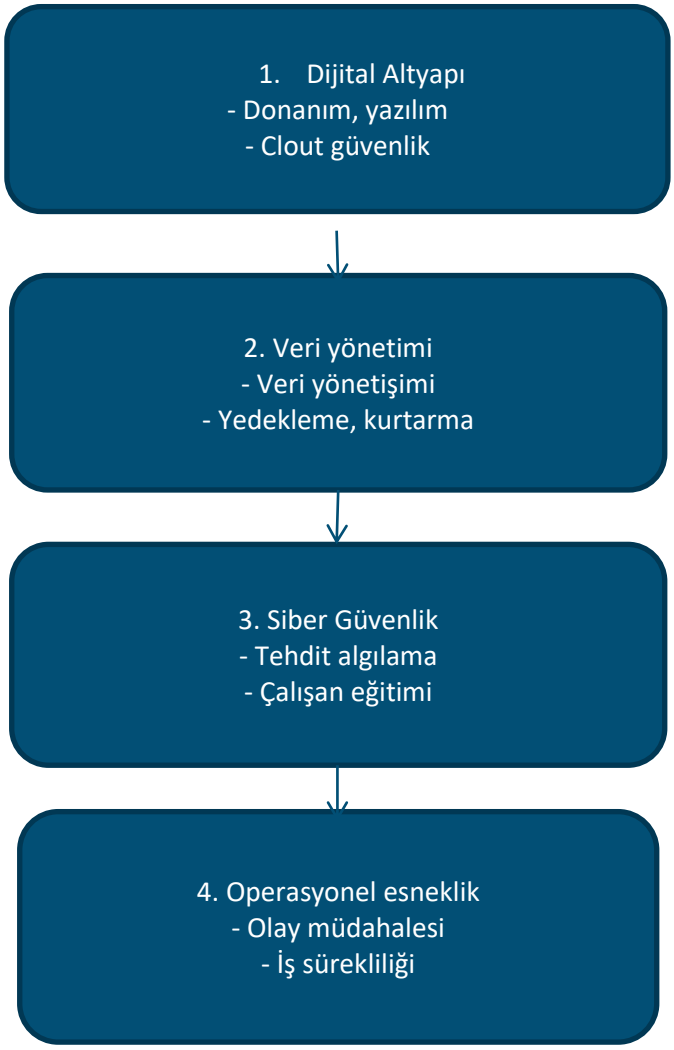
Veri yönetişimi, bir kuruluş içindeki veri varlıklarının yönetimi ve gözetimi anlamına gelir. Verilerin etkin, sorumlu ve etik bir şekilde yönetilmesini sağlamak için veri kalitesi, bütünlüğü ve güvenliğine yönelik politikaların, süreçlerin ve kontrollerin oluşturulmasını içerir.

G) Olaylara müdahale ve iş sürekliliği planlaması

Olay müdahalesi ve iş sürekliliği planlaması, siber güvenlik olaylarına ve aksaklıklarına hazırlanmayı ve bunlara müdahale etmeyi içerir. Startup'lar siber saldırıların, veri ihlallerinin veya diğer aksaklıkların operasyonları ve itibarları üzerindeki etkisini azaltmak için kapsamlı olay müdahale planları ve iş sürekliliği stratejileri geliştirmelidir.

Dolayısıyla dijital hijyen, dijital varlıkların ve operasyonların güvenliğini, verimliliğini ve bütünlüğünü korumayı amaçlayan bir dizi uygulama ve protokolü kapsar. Bu kavramsal çerçeve, startup'ların benzersiz ihtiyaçlarına ve kısıtlamalarına göre uyarlanmış dijital hijyenin temel bileşenlerini tanımlamaktadır.

Girişimler için Dijital Hijyen Kavramsal Çerçevesinin Şeması Şekil 1'de gösterilmektedir.



Şekil 1. Girişimler için Dijital Hijyen Kavramsal Çerçevesinin Şeması

Bu şema, girişimler için Dijital Hijyenin dört ana bileşenini özetlemektedir: Dijital Altyapı, Veri Yönetimi, Siber Güvenlik ve Operasyonel Dayanıklılık. Her bir bileşen, bir startup ortamındaki dijital varlıkların ve operasyonların güvenliğini, verimliliğini ve bütünlüğünü sağlamayı amaçlayan belirli uygulamaları ve protokolleri kapsar.

Dijital altyapı, girişimlerin faaliyetlerini desteklemek ve ürün veya hizmet sunmak için kullandıkları donanım, yazılım ve bulut hizmetlerini kapsar. Bilgisayarlar, sunucular ve ağ ekipmanları gibi cihazların yanı sıra yazılım uygulamaları ve platformları da içerir.

Veri yönetimi, bir girişimdeki veri varlıklarının yönetişimini, depolanmasını ve korunmasını içerir. Verilerin toplanması, depolanması, kullanılması ve paylaşılmasının yanı sıra yasal gerekliliklere uyum ve veri ihlallerine karşı korumayı da kapsar.

Siber güvenlik, dijital varlıkları ve operasyonları kötü amaçlı yazılım, kimlik avı saldırıları ve yetkisiz erişim girişimleri gibi siber tehditlerden korumaya odaklanır. Güvenlik olaylarını tespit etmek, önlemek ve bunlara etkili bir şekilde yanıt vermek için proaktif önlemlerin alınmasını içerir.

Operasyonel esneklik, doğal afetler, siber saldırılar veya sistem arızaları gibi yıkıcı olaylar karşısında iş operasyonlarının devamlılığını ve esnekliğini sağlamayı içerir. Kesinti süresini en aza indirmek ve kritik iş işlevlerini sürdürmek için planlama, hazırlık ve müdahale önlemlerini kapsar.

Şekil 2, dijital hijyen sürecini ve başlangıç faaliyetindeki faktörlerini göstermektedir.

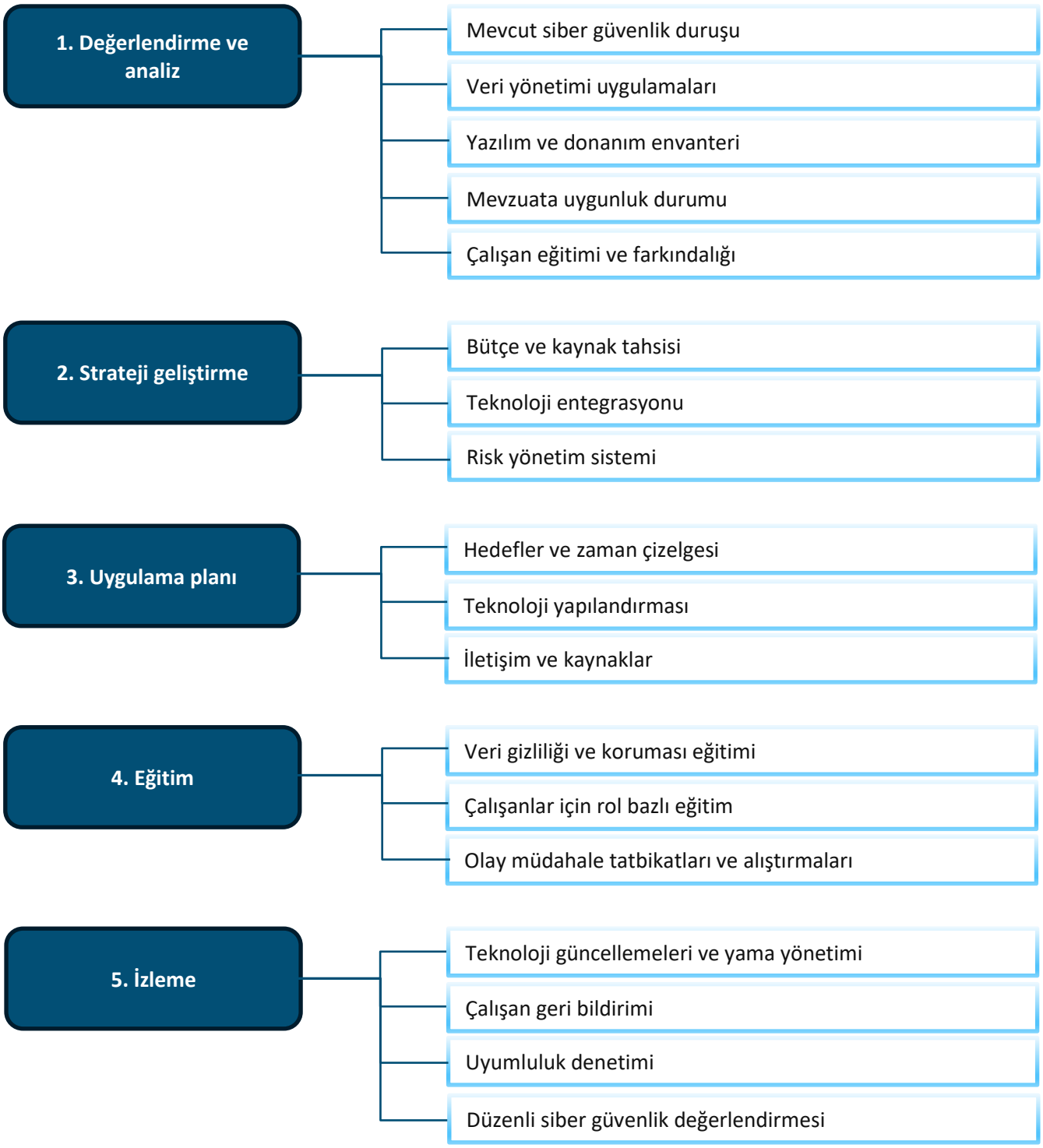
Bu ayrıntılı şekil, bir startup'taki kapsamlı dijital hijyen sürecini göstermekte, değerlendirme ve analizden sürekli izleme ve iyileştirmeye kadar her aşamadaki temel faktörleri ve bileşenleri vurgulamaktadır.

Girişim, dijital altyapısı ve verilerine yönelik potansiyel riskleri ve tehditleri analiz ederek mevcut dijital uygulamalarının ve güvenlik açıklarının kapsamlı bir değerlendirmesini yapar. Değerlendirme bulgularına dayanarak girişim, ihtiyaçlarına ve hedeflerine göre uyarlanmış kapsamlı bir dijital hijyen stratejisi geliştirir ve iyileştirme alanlarına öncelik verir.

Girişim, dijital hijyen önlemlerinin uygulanması için net hedefler ve zaman çizelgeleri tanımlar ve bütçe, personel ve teknoloji dahil olmak üzere kaynakları etkin bir şekilde tahsis eder. Girişim, çalışanlara dijital güvenliğin en iyi uygulamaları konusunda eğitim oturumları ve eğitim materyalleri sağlayarak kurum içinde bir siber güvenlik farkındalığı ve sorumluluğu kültürünü teşvik eder.

Girişim, dijital hijyen çabalarını sürekli olarak izler ve değerlendirir, gelişen tehditlere ve zorluklara uyum sağlamak ve iyileştirme alanlarını belirlemek için düzenli denetimler ve değerlendirmeler yapar.

Sonuç olarak, etkili dijital hijyen uygulamaları, dijital girişimciliğin karmaşık ve dinamik ortamında yol almak isteyen startup'lar için vazgeçilmezdir. Burada özetlenen kavramsal çerçeveyi uygulayarak girişimler dijital altyapılarını güçlendirebilir, veri varlıklarını koruyabilir ve siber güvenlik duruşlarını geliştirebilirler.



Şekil 2. Dijital Hijyen Dijital hijyen süreci ve başlangıçtaki faktörleri

Ünite 2 – “Startup”lar için İyi Dijital Hijyenin gereklilikleri/temelleri

Günümüzün dijital çağında 'startup'lar inovasyonu teşvik etmek, operasyonları kolaylaştırmak ve müşterilere ulaşmak için büyük ölçüde teknolojiye güveniyor. Bununla birlikte, teknolojinin faydaları siber tehditler, veri ihlalleri ve operasyonel aksaklıklar gibi riskleri de beraberinde getiriyor. Bu zorlukların üstesinden gelmek ve uzun vadeli başarı sağlamak için yeni kurulan şirketlerin iyi dijital hijyen uygulamalarına öncelik vermesi gerekir.

İyi dijital hijyen uygulamaları, bir girişimin dijital varlıklarını, altyapısını ve verilerini potansiyel tehditlere, güvenlik açıklarına ve risklere karşı korumayı amaçlayan bir dizi proaktif önlem ve protokolü kapsar.

Startup'lar için iyi bir dijital hijyenin gereklilikleri:

1. Siber tehditlere ve saldırılara karşı koruma

İyi dijital hijyen uygulamalarını sürdürmenin başlıca nedenlerinden biri, girişimleri siber tehditlere ve saldırılara karşı korumaktır. Siber suçların arttığı bir çağda, yeni kurulan şirketler dijital altyapı ve sistemlerindeki açıklardan faydalanmak isteyen kötü niyetli aktörler için başlıca hedeflerdir. Kötü amaçlı yazılım bulaşmaları, kimlik avı dolandırıcılığı, fidye yazılımı saldırıları ve veri ihlalleri gibi siber saldırılar, girişimler için mali kayıplar, itibar zedelenmesi, yasal yükümlülükler ve operasyonel aksaklıklar gibi yıkıcı sonuçlar doğurabilir. Girişimler, sağlam siber güvenlik önlemleri uygulayarak savunmalarını güçlendirebilir ve siber tehditlerin yarattığı riskleri azaltabilir, kritik varlıklarını koruyabilir ve iş sürekliliğini sağlayabilir.

2. Hassas verilerin ve fikri mülkiyetin korunması

Startup'lar genellikle müşteri bilgileri, tescilli teknolojiler, ticari sırlar ve fikri mülkiyet dahil olmak üzere hassas verilerle uğraşır. İyi dijital hijyen uygulamalarının sürdürülmesi, bu hassas bilgilerin yetkisiz erişime, hırsızlığa veya tehlikeye atılmaya karşı korunması için çok önemlidir. Veri ihlalleri ve yetkisiz ifşalar yalnızca mali kayıplara ve yasal yükümlülüklere neden olmakla kalmaz, aynı zamanda müşteri güvenini ve itimadını sarsarak girişimin itibarını ve marka imajını zedeleyebilir. Veri şifreleme, erişim kontrolleri ve veri kaybı önleme tedbirleri uygulayarak girişimler hassas veri varlıklarını koruyabilir ve bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini muhafaza ederek müşterilerin, ortakların ve paydaşların güvenini koruyabilir.

3. Operasyonel verimliliğin ve üretkenliğin artırılması

İyi dijital hijyen uygulamaları, girişimlerde operasyonel verimliliğin ve üretkenliğin artırılmasına da katkıda bulunur. Güncelliğini yitirmiş yazılımlar, yamalanmamış sistemler ve verimsiz dijital iş akışları üretkenliği

engelleyebilir, işbirliğini sekteye uğratabilir ve işletmenin büyümesini sekteye uğratabilir. Girişimler dijital altyapılarını düzenli olarak koruyup güncelleyerek performansı optimize edebilir, süreçleri kolaylaştırabilir ve darboğazları ortadan kaldırarak çalışanların daha verimli ve etkili çalışmasını sağlayabilir. Ayrıca, otomasyon, bulut teknolojileri ve dijital araçlardan yararlanarak girişimler iş akışlarını düzene sokabilir, rutin görevleri otomatikleştirebilir ve karar alma süreçlerini iyileştirerek inovasyonu ve pazardaki rekabet gücünü artırabilir.

4. Mevzuata uygunluğun ve yasal yükümlülüklerin sağlanması

Düzenleyici gerekliliklere ve yasal yükümlülüklere uyum, iyi dijital hijyen uygulamalarını sürdürmenin bir diğer kritik yönüdür. Çeşitli sektörlerde faaliyet gösteren startup'lar veri gizliliği, güvenliği ve korunmasını düzenleyen sayısız yasa, yönetmelik ve uyum standartlarına tabidir. Bu düzenlemelere uyulmaması ciddi cezalara, para cezalarına ve yasal sonuçlara yol açarak startup'ın yaşayabilirliğini ve itibarını tehlikeye atabilir. GDPR, HIPAA, PCI DSS veya SOX gibi düzenleyici gerekliliklere bağlı kalarak girişimler etik iş uygulamalarına bağlılıklarını gösterebilir, müşterilerin ve paydaşların güvenini kazanabilir ve yasal ve finansal riskleri azaltabilir.

5. Yenilikçiliğin teşvik edilmesi

Son olarak, iyi dijital hijyen uygulamalarının sürdürülmesi, startup'larda inovasyonun ve uyarlanabilirliğin teşvik edilmesi için elzemdir. Teknolojik gelişmelerin ve piyasa aksaklıklarının olağan hale geldiği günümüzün dijital ekonomisinde, girişimler rekabetçi bir ortamda başarılı olmak için çevik, esnek ve uyarlanabilir kalmalıdır. Yeni teknolojileri benimseyerek, dijital dönüşümü kucaklayarak ve sürekli gelişim ve öğrenme kültürünü geliştirerek startup'lar kendilerini uzun vadeli başarı ve sürdürülebilirlik için konumlandırabilir, inovasyonu teşvik edebilir ve müşterileri ve paydaşları için değer yaratabilir.

Özetle, iyi dijital hijyen uygulamalarını sürdürmek, uzun vadeli başarı, büyüme ve esneklik arayan girişimler için vazgeçilmezdir.

.

Ünite 3 - Dijital Hijyenin Önemi

İyi bir dijital hijyen sağlamanın önemi yadsınamaz. Hassas verilerin korunmasından siber tehditlerin azaltılmasına kadar, dijital hijyen uygulamaları hem bireyler hem de kuruluşlar için çok önemlidir. Bu vaka çalışmasında, dijital hijyenin önemini gerçek hayattan bir örnek üzerinden inceleyerek güvenlik, üretkenlik ve genel refah üzerindeki etkisini vurguluyoruz.

Dijital hijyenin önemini anlamak için bazı dijital hijyen uygulamalarına göz atın.

1. İşletmeler için son teknoloji yazılım çözümleri geliştirme konusunda uzmanlaşmış, Silikon Vadisi merkezli dinamik bir startup olan TechGenius ile tanışın. 2015 yılında kurulan TechGenius, en iyi yetenekleri çekerek ve yüksek profilli müşterileri güvence altına alarak teknoloji sektöründe hızla öne çıktı. Ancak şirket faaliyetlerini ve iş gücünü genişlettikçe dijital altyapısını yönetme ve dijital varlıklarını koruma konusunda yeni zorluklarla karşılaştı.

TechGenius, birçok startup gibi, inovasyon ve verimliliğin her şeyden önemli olduğu hızlı tempolu bir ortamda faaliyet gösteriyordu. Ancak günlük operasyonların koşuşturmacası arasında şirket dijital hijyen uygulamalarına öncelik vermeyi ihmal etti. Çalışanların sıklıkla zayıf parolalar kullanması, yazılımları düzenli olarak güncellememesi ve temel güvenlik protokollerini göz ardı etmesi, şirketi kimlik avı saldırıları ve veri ihlalleri gibi siber tehditlere karşı savunmasız bıraktı.

Dijital hijyenin kritik öneminin farkına varan TechGenius, siber güvenlik ve veri yönetimi yaklaşımını yenilemek için bir yolculuğa çıktı. Şirket, çalışanlarını eğitmeyi, en iyi uygulamaları hayata geçirmeyi ve güvenlik duruşunu güçlendirmeyi amaçlayan kapsamlı bir dijital hijyen girişimi başlattı.

TechGenius'un dijital hijyen girişimi birkaç temel bileşenden oluşuyordu:

1. Çalışan eğitimi ve farkındalığı. Şirket, çalışanlarını dijital hijyenin önemi konusunda eğitmek için kapsamlı eğitim oturumları düzenledi. Kapsanan konular arasında parola yönetimi, e-posta güvenliği, güvenli tarama uygulamaları ve veri koruma düzenlemeleri yer aldı. İnteraktif atölye çalışmaları ve çevrimiçi modüller sayesinde çalışanlar siber güvenlik riskleri ve bu riskleri azaltmadaki rolleri hakkında daha derin bir anlayış kazandı.

2. Politika geliştirme ve uygulama. TechGenius, çalışan davranışlarını yönetmek ve sektör standartlarına uygunluğu sağlamak için sağlam dijital hijyen politikaları ve prosedürleri geliştirdi. Bu politikalar parola karmaşıklığı, yazılım güncellemeleri, erişim kontrolleri ve olay müdahale protokolleri gibi alanları ele almıştır. Şirket, hesap verebilirliği güçlendirmek amacıyla bu politikalara uyulup uyulmadığını izlemek için düzenli denetimler ve yaptırım mekanizmaları uygulamıştır.

3. Teknolojik çözümler. Eğitim ve politika önlemlerine ek olarak TechGenius dijital hijyen uygulamalarını geliştirmek için teknolojik çözümlere yatırım yapmıştır. Buna çok faktörlü kimlik doğrulama, şifreleme teknolojileri, uç nokta güvenlik yazılımı ve ağ izleme araçlarının uygulanması dahildir. Şirket bu teknolojilerden yararlanarak siber tehditlere karşı savunmasını güçlendirmiş ve dijital altyapısını korumuştur.

TechGenius'un dijital hijyen girişiminin uygulanması önemli sonuçlar verdi:

A. Geliştirilmiş güvenlik duruşu. TechGenius dijital hijyene öncelik vererek güvenlik duruşunu güçlendirdi ve siber tehdit riskini azalttı. Kimlik avı saldırıları ve veri ihlalleri gibi olayların sıklığı azaldı ve şirketin operasyonları ve itibarı üzerindeki potansiyel etki en aza indirildi.

B. Artan üretkenlik. Daha az güvenlik olayıyla uğraşmak zorunda kalan çalışanlar temel sorumluluklarına daha fazla odaklanabildi ve bu da kurum genelinde üretkenliğin ve verimliliğin artmasına yol açtı. Dijital iş akışlarını düzene sokarak ve kesinti sürelerini en aza indirerek TechGenius daha iyi sonuçlar elde etti ve müşterilerine üstün sonuçlar sundu.

C. Korunan itibar. Güvenilir bir yazılım çözümleri sağlayıcısı olarak TechGenius'un itibarı, müşteri verilerini koruma ve yüksek güvenlik standartlarını sürdürme becerisine bağlıdır. Şirket, dijital hijyene bağlılığını göstererek müşterilerinin güvenini ve itimadını kazanmış ve giderek daha rekabetçi hale gelen bir pazarda kendisini güvenilir bir ortak olarak konumlandırmıştır.

D. Maliyet Tasarrufu. Dijital hijyene yatırım yapmak başlangıçta maliyetli olsa da, uzun vadeli faydaları masraflarından çok daha fazladır. TechGenius, siber güvenlik olaylarının azalması, uyum cezalarının düşmesi ve operasyonel verimliliğin artması sayesinde maliyet tasarrufu elde etti. Şirket, güvenlik açıklarını proaktif bir şekilde ele alarak veri ihlalleri ve mevzuata uyumsuzlukla ilişkili potansiyel olarak maliyetli yansımalardan kaçındı.

TechGenius vakası, günümüzün dijital ortamında dijital hijyenin kritik öneminin altını çizmektedir. TechGenius, siber güvenlik eğitimine, politika geliştirmeye ve teknolojik çözümlere öncelik vererek siber tehditleri azaltmayı, üretkenliği artırmayı ve itibarını ve kar hanesini korumayı başardı. Bu gerçek hayat örneği, kuruluşları gelişen siber risklere karşı güvence altına alma ve sürdürülebilir büyüme ve başarı sağlama konusunda dijital hijyenin dönüştürücü gücünün bir kanıtıdır.

Dijital hijyen uygulamalarının önemini gösteren bir başka örnek de SecureHealth vakasıdır.

SecureHealth, tıbbi kayıtların yönetilme ve erişilme biçiminde devrim yaratan bir sağlık teknolojisi girişimidir. Hasta bakımını kolaylaştırmak ve sağlık hizmeti sonuçlarını iyileştirmek için tasarlanmış bulut tabanlı bir platforma sahip olan SecureHealth, sağlık sektöründe hızla ilgi görmeye başlamıştır. Bununla

birlikte, platformunun hızlı büyümesi ve benimsenmesinin ortasında, şirket hasta verilerinin güvenliğini ve gizliliğini sağlamada önemli zorluklarla karşılaşmaktadır.

Sağlık kuruluşları, işledikleri verilerin hassas yapısı nedeniyle siber saldırılar için başlıca hedeflerdir. SecureHealth, hasta gizliliğinin korunması ve mevzuata uygunluğun sürdürülmesinde dijital hijyenin kritik öneminin farkındadır. Bununla birlikte, sağlık hizmetleri BT sistemlerinin karmaşıklığı ve sürekli gelişen tehdit ortamı nedeniyle şirket, siber güvenlik risklerini ele alma konusunda tetikte ve proaktif olmalıdır.

SecureHealth, dijital hijyen konusunda proaktif bir yaklaşım benimseyerek sağlık sektörünün kendine özgü ihtiyaçlarına göre uyarlanmış kapsamlı bir siber güvenlik programı uygulamaktadır. Şirket aşağıdaki temel bileşenlere öncelik vermektedir:

1. Veri şifreleme ve erişim kontrolleri. SecureHealth, hasta verilerini hem dinlenme hem de aktarım sırasında şifreleyerek hassas bilgilerin yetkisiz erişime karşı korunmasını sağlar. Hasta kayıtlarına erişimi yalnızca yetkili sağlık uzmanlarıyla kısıtlamak için erişim kontrolleri uygulanarak veri ihlali riski en aza indirilir.

2. Düzenli güvenlik denetimleri ve sızma testleri. SecureHealth, sistemlerindeki ve altyapısındaki güvenlik açıklarını belirlemek için düzenli güvenlik denetimleri ve sızma testleri gerçekleştirir. Şirket, güvenlik zayıflıklarını proaktif olarak belirleyip gidererek siber tehditlere karşı savunmasını güçlendirir ve HIPAA gibi sağlık hizmetleri düzenlemelerine uyum sağlar.

3. Çalışan eğitimi ve farkındalığı. SecureHealth, hasta verilerinin korunmasında dijital hijyenin önemini vurgulayarak tüm çalışanlara kapsamlı siber güvenlik eğitimi vermektedir. Çalışanlar, güvenlik tehditlerini nasıl tanıyacaklarını ve bunlara nasıl yanıt vereceklerini, günlük iş akışlarında güvenli uygulamaları nasıl uygulayacaklarını ve şirket politikalarına ve prosedürlerine nasıl uyacaklarını öğrenirler.

SecureHealth'in dijital hijyen girişimlerinin uygulanması somut sonuçlar vermiştir:

A. Korunan hasta verileri. Dijital hijyene öncelik veren SecureHealth, hasta verilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlayarak hem sağlık hizmeti sağlayıcıları hem de hastalar arasında güven ve itimadı teşvik eder.

B. Düzenlemelere uygunluk. SecureHealth, hasta gizliliğini koruma ve veri güvenliği ve gizliliği için endüstri standartlarını karşılama konusundaki kararlılığını göstererek HIPAA gibi sağlık hizmetleri düzenlemelerine uymayı sürdürür.

C. Azaltılmış veri ihlali riski. Güçlü siber güvenlik önlemleri sayesinde SecureHealth, veri ihlalleri ve diğer güvenlik olayları riskini en aza indirerek itibarını korur ve olası mali ve yasal sonuçları en aza indirir.

SecureHealth'in deneyimi, risklerin yüksek olduğu ve güvenlik ihlallerinin sonuçlarının ağır olabileceği sağlık sektöründe dijital hijyenin kritik önemini vurgulamaktadır. SecureHealth, veri şifreleme, erişim kontrolleri, düzenli denetimler ve çalışan eğitimi gibi siber güvenlik önlemlerine öncelik vererek hasta verilerinin güvenliğini ve bütünlüğünü sağlar ve sonuçta hasta bakımının ve sonuçlarının iyileştirilmesine katkıda bulunur.

Dijital hijyenin önemini kavramak için ek dijital hijyen uygulamalarını incelemeyi düşünün.

FinTech Innovations, yenilikçi dijital bankacılık çözümleriyle finansal hizmetler sektörünü altüst eden bir girişimdir. Blok zinciri ve yapay zeka gibi en son teknolojilerden yararlanan FinTech Innovations, hem tüketicilere hem de işletmelere güvenli, kullanıcı dostu bankacılık hizmetleri sunmaktadır. Ancak şirket büyüdükçe ve müşteri tabanını genişlettikçe, platformunun güvenliğini ve istikrarını tehdit eden artan siber güvenlik riskleriyle karşı karşıya kalmaktadır.

Finans kurumları, sahip oldukları değerli finansal veriler nedeniyle siber saldırılar için birincil hedeflerdir. FinTech Innovations, müşterilerinin ve iş ortaklarının güvenini ve itimadını korumada dijital hijyenin öneminin farkındadır. Bununla birlikte, finansal işlemlerin karmaşıklığı ve siber tehditlerin gelişen doğası nedeniyle, şirket dijital varlıklarını ve altyapısını korumak için tetikte ve proaktif olmalıdır.

FinTech Innovations, siber güvenlik risklerini ele almak ve platformunu korumak için sağlam bir dijital hijyen programı uygulamaktadır. Şirket aşağıdaki temel girişimlere odaklanmaktadır:

1. Güvenli kimlik doğrulama ve yetkilendirme. FinTech Innovations, kullanıcıların kimliğini doğrulamak ve hesaplara ve işlemlere yetkisiz erişimi önlemek için biyometrik kimlik doğrulama ve çok faktörlü kimlik doğrulama gibi güçlü kimlik doğrulama mekanizmaları uygular.

2. Gerçek zamanlı dolandırıcılık tespiti. FinTech Innovations, dolandırıcılık faaliyetlerini gerçek zamanlı olarak tespit etmek ve önlemek için gelişmiş analitik ve makine öğrenimi algoritmalarından yararlanır. Şirket, işlem modellerini ve kullanıcı davranışlarını analiz ederek şüpheli faaliyetleri belirleyebilir ve dolandırıcılık risklerini azaltmak için proaktif önlemler alabilir.

3. Sürekli izleme. FinTech Innovations, güvenlik olaylarını derhal tespit etmek ve bunlara yanıt vermek için sistemlerini ve ağlarını sürekli olarak izler. Şirket, şüpheli faaliyetleri izleyen, güvenlik uyarılarını araştıran ve potansiyel tehditleri ele almak için zamanında düzeltme eylemleri uygulayan özel bir siber güvenlik uzmanları ekibi istihdam etmektedir.

FinTech Innovations'ın dijital hijyen girişimlerinin uygulanması önemli sonuçlar doğurmuştur:

A. Artan müşteri güveni. FinTech Innovations, dijital hijyene öncelik vererek müşteri verilerini ve finansal varlıkları koruma, kullanıcıları ve paydaşları arasında güven ve itimat oluşturma konusundaki kararlılığını göstermektedir.

B. Azaltılmış dolandırıcılık ve güvenlik olayları. Gelişmiş dolandırıcılık tespit mekanizmaları ve sürekli izleme ile FinTech Innovations, dolandırıcılık ve güvenlik olayları riskini en aza indirerek platformunun ve işlemlerinin güvenliğini ve bütünlüğünü sağlar.

C. İş sürekliliği ve esneklik. FinTech Innovations, siber güvenlik risklerini proaktif bir şekilde ele alarak siber tehditlere ve aksaklıklara karşı dayanıklılığını artırır ve finansal hizmetlerin müşterilerine ve ortaklarına kesintisiz bir şekilde sunulmasını sağlar.

FinTech Innovations'ın deneyimi, güvenlik ve güvenin çok önemli olduğu finansal hizmetler sektöründe dijital hijyenin kritik öneminin altını çizmektedir. FinTech Innovations, güvenli kimlik doğrulama, dolandırıcılık tespiti ve sürekli izleme gibi sağlam siber güvenlik önlemleri uygulayarak platformunun güvenliğini ve istikrarını sağlamakta ve nihayetinde müşterileri için daha güvenli ve emniyetli bir dijital bankacılık deneyimine katkıda bulunmaktadır

Bu örnekler, sağlık ve finans gibi çeşitli sektörlerde hassas verilerin korunması, mevzuata uygunluğun sürdürülmesi ve siber tehditlere karşı korunmada dijital hijyenin hayati rolünü göstermektedir. Dijital hijyene öncelik vermek, riskleri azaltmak, güven oluşturmak ve günümüzün dijital ortamında sürdürülebilir büyüme ve başarı sağlamak isteyen kuruluşlar için çok önemlidir.

Ünite 4 - 1 Yeni kurulan şirketlerden iyi uygulamalar

Etkili tehdit tanımlama ve önleyici tedbirleri göstermek için, personel için siber güvenlik eğitimini vurgulayan bir örneği inceleyeceğiz. Bu örnek, dijital güvenlik önlemlerinin güçlendirilmesinde çalışan eğitiminin kritik rolünün altını çizmeye hizmet etmektedir.

CyberSec Avrupa

Bağlam

CyberSec Europe, Berlin, Almanya merkezli, küçük ve orta ölçekli işletmeler (KOBİ'ler) için güvenlik çözümleri sağlama konusunda uzmanlaşmış bir siber güvenlik girişimidir. 2017 yılında kurulan CyberSec Europe, kısa sürede Avrupa pazarında güvenilir bir siber güvenlik hizmetleri sağlayıcısı olarak kendini kanıtladı. Şirket büyüdükçe ve müşteri tabanını genişlettikçe, çalışanları için siber güvenlik eğitiminin kritik öneminin farkına vardı**.**

Yetenekli siber güvenlik uzmanlarından oluşan bir ekibe sahip olmasına rağmen CyberSec Europe, çalışanlarının siber güvenlikle ilgili en iyi uygulamalar konusundaki farkındalığını artırma ihtiyacı olduğunu tespit etti. Siber tehditlerin giderek karmaşıklaşması ve uzaktan çalışma düzenlemelerinin benimsenmesiyle birlikte, kimlik avı saldırıları ve veri ihlalleri gibi güvenlik olayları riski artıyordu. CyberSec Europe, çalışanlarını siber güvenlik riskleri ve protokolleri konusunda eğitmenin, güvenilir bir siber güvenlik sağlayıcısı olarak itibarını korumak için çok önemli olduğunu anladı.

Çözüm

CyberSec Europe, tüm çalışanları için tehdit algılama, olaylara müdahale ve Genel Veri Koruma Yönetmeliği (GDPR) gibi veri koruma düzenlemelerine uyum gibi temel alanlara odaklanan kapsamlı bir güvenlik eğitim programı uyguladı. Eğitim programı etkileşimli, ilgi çekici ve CyberSec Europe'un işgücünün özel ihtiyaçlarına göre tasarlandı.

Güvenlik eğitim programı üç ay boyunca şirket genelinde uygulandı. Program, şirket içi siber güvenlik uzmanları ve dış danışmanlar tarafından yönetilen bir dizi atölye çalışması, web semineri ve uygulamalı alıştırmadan oluşuyordu. Eğitim programında ele alınan konular şunlardır:

- ✓ Kimlik avı e-postalarını tespit etme ve yanıtlama
- ✓ Güçlü parolalar oluşturma ve yönetme
- ✓ Siber saldırıların yaygın belirtilerini tanıma
- ✓ Hassas verilerin korunması ve GDPR uyumluluğunun sağlanması
- ✓ Güvenlik olaylarını bildirmek ve olay müdahale prosedürlerini takip etmek.

CyberSec Europe, katılımı ve bağlılığı teşvik etmek için çalışanları eğitim modüllerini tamamlamaya teşvik etti ve güvenlik farkındalığı egzersizlerinde örnek performans için ödüller sundu. Şirket ayrıca çalışanlara siber güvenlik araçlarına ve çevrimiçi kaynaklara erişim gibi sürekli destek ve kaynaklar sağladı.

Düzenli güvenlik eğitimlerinin uygulanması CyberSec Europe için olumlu sonuçlar vermiştir:

1. Artan güvenlik farkındalığı. Çalışanlar siber güvenlik riskleri konusunda daha dikkatli ve bilgili hale gelerek güvenlik olaylarının ve veri ihlallerinin azalmasını sağladı.

2. Geliştirilmiş güvenlik uygulamaları. Çalışanlar, güçlü parolalar kullanmak, hassas verileri şifrelemek ve şüpheli faaliyetleri derhal bildirmek gibi siber güvenlik alanındaki en iyi uygulamaları benimsedi.

3. Artan müşteri güveni. CyberSec Europe'un siber güvenlik eğitimi konusundaki kararlılığı, müşteri verilerini ve gizliliğini korumaya olan bağlılığını göstererek müşterileri arasında güven ve güvenilirliği artırdı.

4. Uyumluluk hazırlığı. CyberSec Europe, çalışanlarını GDPR gereklilikleri ve diğer düzenleyici standartlar hakkında eğiterek uyumluluk duruşunu iyileştirdi ve düzenleyici cezalar riskini en aza indirdi.

CyberSec Europe'un siber güvenlik eğitimine yönelik proaktif yaklaşımı, Avrupa'daki girişimler için düzenli güvenlik eğitiminin önemini vurguluyor. CyberSec Europe, çalışanlarının farkındalığına ve güçlendirilmesine yatırım yaparak siber güvenlik savunmasını güçlendirmeyi, riskleri azaltmayı ve müşterileriyle güven tesis etmeyi başardı. Bu gerçek hayat örneği, güvenlik eğitiminin dijital hijyeni artırmadaki ve Avrupa pazarındaki girişimleri siber tehditlere karşı korumadaki etkinliğini vurgulamaktadır.

İyi dijital hijyen uygulamalarının sağlanması, Avrupa'daki girişimlerin günümüzün dijital ortamında başarılı olması için çok önemlidir. Siber tehditlerin, veri ihlallerinin ve yasal gerekliliklerin artan yaygınlığı, siber güvenlik, veri koruma ve uyumluluk çabalarına öncelik vermenin önemini vurgulamaktadır. Girişimler, sağlam dijital hijyen önlemleri uygulayarak dijital varlıklarını koruyabilir, hassas verileri muhafaza edebilir ve müşteriler, iş ortakları ve paydaşlarla güven tesis edebilir. Bununla birlikte, iyi bir dijital hijyene ulaşmak ve bunu sürdürmek, uyumlu bir çaba, sürekli dikkat ve sürekli iyileştirme taahhüdü gerektirir.

Avrupa'daki Startup'ların Dijital Hijyeninin İyileştirilmesi için Öneriler

- ✓ Girişimlerin siber güvenlik duruşu, veri yönetimi protokolleri ve mevzuata uygunluk durumu dahil olmak üzere dijital hijyen uygulamalarını düzenli olarak değerlendirmeleri önerilir. Bu, güvenlik açıklarının, boşlukların ve iyileştirme alanlarının belirlenmesine yardımcı olacaktır.
- ✓ Değerlendirme bulgularına dayanarak, startup'ların kendi özel ihtiyaçlarına, hedeflerine ve risk profillerine göre uyarlanmış kapsamlı dijital hijyen stratejileri geliştirmeleri tavsiye edilir. Stratejiler siber güvenlik, veri koruma, uyumluluk ve olaylara müdahale gibi kilit alanları ele almalıdır.

✓ Girişimlerin dijital altyapılarını siber tehditlerden, kötü amaçlı yazılımlardan ve veri ihlallerinden korumak için siber güvenlik teknolojilerine ve çözümlerine yatırım yapmaları önerilir. Bunlar arasında güvenlik duvarları, antivirüs yazılımları, şifreleme teknolojileri ve izinsiz giriş tespit sistemleri sayılabilir.

✓ Startup'lar şifreleme, erişim kontrolleri, veri yedekleme ve kurtarma mekanizmaları dahil olmak üzere sağlam veri yönetimi protokolleri uygulayarak veri koruma ve gizliliğe öncelik vermelidir. GDPR gibi düzenlemelere uyum, kişisel verileri işleyen girişimler için çok önemlidir.

✓ Girişimlerin, potansiyel riskleri, en iyi uygulamaları ve iyi bir dijital hijyen sağlamaya yönelik prosedürleri anlamalarını sağlamak için çalışanlar arasında siber güvenlik farkındalığını ve eğitimini teşvik etmeleri tavsiye edilir. Düzenli eğitim oturumları, farkındalık kampanyaları ve oltalama simülasyonları siber güvenlik farkındalığını güçlendirmeye yardımcı olabilir.

✓ Startup'lar siber güvenlik olaylarına, veri ihlallerine veya diğer acil durumlara etkili bir şekilde yanıt vermek için olay müdahale planları geliştirmeli ve uygulamalıdır. Planlar, olayların tespit edilmesi, kontrol altına alınması ve hafifletilmesine yönelik rolleri, sorumlulukları ve prosedürleri ana hatlarıyla belirlemelidir.

✓ İyi bir dijital hijyen sağlamak için sürekli izleme ve değerlendirme şarttır. Girişimlerin dijital hijyen önlemlerinin etkinliğini düzenli olarak değerlendirmeleri, denetimler ve incelemeler yapmaları ve ortaya çıkan tehditleri ve zorlukları ele almak için gerekli ayarlamaları yapmaları önerilir.

✓ Startup'lar, sektörlerini etkileyen en son siber güvenlik tehditleri, trendleri ve düzenlemeleri hakkında bilgi sahibi olmalıdır. Siber güvenlik haberlerini düzenli olarak izlemek, sektör forumlarına katılmak ve siber güvenlik uzmanlarıyla işbirliği yapmak, girişimlerin gelişen tehdit ve risklerin bir adım önünde olmalarına yardımcı olabilir.

Özetle, dijital hijyen uygulamalarının iyileştirilmesi Avrupa'daki startup'ların dijital varlıklarını korumaları, riskleri azaltmaları ve paydaşlarının güvenini sürdürmeleri için elzemdir. Kapsamlı stratejiler uygulayarak, siber güvenlik teknolojilerine yatırım yaparak, farkındalığı artırarak ve değişen tehditleri sürekli izleyip bunlara uyum sağlayarak girişimler dijital dayanıklılıklarını güçlendirebilir ve rekabet ortamında başarılı olabilirler.

Önemli Çıkarımlar

- Girişimlerin, farkındalık yaratmak ve siber tehditleri tanıyıp bunlara etkili bir şekilde yanıt vermelerini sağlamak için çalışanlarına siber güvenlik eğitimi vermeye öncelik vermeleri önerilir. Eğitim programları kimlik avı farkındalığı, parola yönetimi ve olay müdahale protokolleri gibi konuları kapsamalıdır.
- Sağlam dijital hijyen politikaları ve prosedürleri oluşturmak, girişimlerde siber güvenlik kültürünü teşvik etmek için çok önemlidir. Parola karmaşıklığı, yazılım güncellemeleri, erişim kontrolleri ve veri koruma düzenlemeleri gibi alanları ele alan politikalar geliştirilmesi tavsiye edilir.
- Düzenli denetimler ve yaptırım mekanizmaları, startup'larda uyum ve hesap verebilirliğin sağlanmasına yardımcı olur. Dijital hijyen politika ve prosedürlerine uyumu izlemek için düzenli denetimler yapılması ve yaptırım mekanizmalarının uygulanması tavsiye edilir.
- Startup'lar dijital hijyen uygulamalarını geliştirmek için teknolojik çözümlere yatırım yapmalıdır. Bu, siber tehditlere karşı savunmayı güçlendirmek için çok faktörlü kimlik doğrulama, şifreleme teknolojileri, uç nokta güvenlik yazılımı ve ağ izleme araçları gibi siber güvenlik araçlarının kullanılmasını içerir.
- Düzenleyici gerekliliklere ve sektör standartlarına uyum, startup'ların etik iş uygulamalarına bağlılıklarını göstermeleri ve yasal ve mali yansımalara karşı korunmaları için kritik önem taşır. Startup'lar veri gizliliği, güvenliği ve bütünlüğünü korumak için GDPR, HIPAA, PCI DSS veya SOX gibi düzenlemelere uymalıdır.
- Dijital hijyen kavramı, siber güvenlik, bilgi yönetimi, insan faktörleri, örgütsel davranış ve uyum teorisi dahil olmak üzere çeşitli disiplinlerden gelen içgörüleri bütünleştirmektedir. Girişimler bu perspektiflerden yararlanarak siber güvenlik ve veri korumanın karmaşık zorluklarını etkili bir şekilde ele almak için yaklaşımlar geliştirebilir.

Referanslar:

1. CyberSec Europe https://www.cyberseceurope.com/
2. FinTech Yenilikleri https://www.fintechinnovation.no/
3. Ncubukezi T., Mwansa L. Covid-19 Pandemisi Sırasında İyi Bir Siber Hijyen Sağlamak İçin İşletmeler Tarafından Kullanılan En İyi Uygulamalar. Journal of Internet Technology and Secured Transactions (JITST), Cilt 9, Sayı 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. Siber hijyen: Kavram, ölçümü ve ilk testleri. Decision Support Systems, Cilt 128, 2020, https://doi.org/10.1016/j.dss.2019.113160.
7. Yegen, C., Kirik, A.M., Çetinkaya, A. (2023). Covid-19 Pandemisi Sırasında Sürdürülebilirlik, Dijital Güvenlik ve Siber Hijyen. İçinde: Mondal, S.R., Yegen, C., Das, S. (eds) New Normal in Digital Enterprises. Palgrave Macmillan, Singapur. https://doi.org/10.1007/978-981-19-8618-5_5

Modül 2 - Dijital Hijyen Araçları ve Günlük Rutinlere Entegrasyon

Ünite 1- Girişimler için En İyi Dijital Hijyen Araçları

Birbirine bağlı bir dünya, daha geniş ve daha karmaşık dijital tehdit risklerini beraberinde getiriyor. Bu nedenle start-up'ların değerli varlıklarını ve gizli bilgilerini korumak için siber güvenliğe büyük önem vermeleri her zamankinden daha önemlidir. Bu ünitede, start-up'ların çevrimiçi güvenliklerini iyileştirmek için üstlenmeleri gereken bazı temel stratejiler ve uygulamalar hakkında bilgi edineceksiniz. Bunlar güçlü parolalar oluşturmaktan kapsamlı veri yedekleme çözümleri uygulamaya kadar uzanmaktadır. Bu kılavuz size start-up'ların çevrimiçi ortamda güvende kalmak için bilmesi gereken bilgi ve araçları sağlayacaktır. Bu ünite, dijital hijyen stratejiniz için güçlü bir temel oluşturmanıza ve dijital varlıklarınızı etkili bir şekilde korumanıza yardımcı olacak temel ilkeleri gözden geçirecek ve bir dizi öneri sunacaktır.

İyi Parola Hijyenini Sürdürmek: Temel Bilgiler

Ticketmaster, Ocak 2021'de rakip şirketin eski bir çalışanının kimlik bilgilerini kullanarak Ticketmaster'ın rakibinin bilgisayarlarına gizlice erişmesini sağlamasının ardından rakip şirketin bilgisayar sistemlerini hacklediği gerekçesiyle dava edildi. ABD Savcı Vekili DuCharme, "Ticketmaster çalışanlarının, yasadışı yollardan elde edilen şifreler aracılığıyla iş bilgilerini çalmak için birçok kez rakibin bilgisayarlarına izinsiz olarak yasadışı bir şekilde eriştiğini" belirtti. Bu tekil vaka, Ticketmaster'ın Bilgisayar Sahtekârlığı ve Suistimal Yasası hükümleri uyarınca 10 milyon dolar nakit cezaya çarptırılmasına yol açmıştır. (Jones, 2022). Google Cloud'un 2023 Tehdit Ufukları Raporu, güvenlik ihlallerinin %86'sının çalıntı kimlik bilgilerinin kullanımını içerdiğini ve kimlik bilgisi sorunlarının ihlallerin altında yatan nedenlerin %60'ından fazlasından sorumlu olduğunu göstermektedir - daha güçlü kurumsal kimlik yönetimi kanatlarının çözülmesine yardımcı olabileceği sorunlar. (Keszthely, 2013)'e göre başkasının şifresini ele geçirme eylemi dört temel yolla gerçekleştirilebilir:

1- Varsayılan kelimeler: Bilgisayarlar ve uygulamalar yerleşik varsayılan şifrelere sahiptir. Bilgisayar ve hesap şifreleri boş olabilir veya "123456", "asdfgh" ve "password" gibi ayrı bir ortak kelime kümesinin parçası olabilir.

2- Giriş adı ve şifreler arasındaki bağlantı: Parola tahmini veya mantığı, saldırganların kullanıcı adı ve parolayı sistematik olarak tahmin etmek için zaman ayırmasıdır. Kullanıcı, saldırganın kullanıcı adı ve şifreyi tahmin etmesine yardımcı bile olabilir. Bazı örnekler "password", "login-login", "qwerty" ve "letmein "dir.

3- Sözlük yöntemi: Hackerlar bazı genel şifreleri toplayacak ve bunları listeden seçecektir. Bunları teker teker indireceklerdir çünkü araçlar çevrimdışı çalışmaktadır ve daha yavaş çalıştıklarında başarılı olma olasılıkları daha yüksektir. Buna ek olarak, internet bağlantısı olmadan da her bir ipucunu test etme fırsatına sahip olacaklardır.

Şifre hırsızlığından kaynaklanan zararlardan kaçınmak için güçlü, güvenli şifrelerin seçimine öncelik vermek gerekir. (Kato & Klyuev, 2013) güçlü parolalar oluşturmak için önerilen bazı ipuçlarını önerir:

- **Büyük Harf ve Noktalama İşaretleri Kullanın:** Daha güçlü bir parola oluşturmak için büyük harfleri ve noktalama işaretlerini kullanın.
- **Karıştırın:** Daha güvenli parolalar oluşturmak için hem harfleri hem de sayıları entegre edin.
- **Yaygın Bilgilerden Kaçının**: Şifrelerde kolayca tahmin edilebilecek kelimeler ve kişisel bilgi detayları kullanmaktan kaçının.
- **Daha Uzun Parolaları Düşünün:** Hatırlaması kolay olan daha uzun şifreleri hedefleyin.
- **Parola Yöneticilerini Kullanın**: LastPass gibi şifreleri güvenli bir şekilde saklamak için tasarlanmış programları kullanın.
- **Benzersiz Şifreler**: Farklı hesaplar için farklı şifreler oluşturun.

Bireysel olarak güvenli parola alışkanlıkları edinmenin yanı sıra, şirketlerin de parola güvenliğini artırmaya odaklanan politikalar uygulaması gerekmektedir. (Inglesant & Sasse, 2010) kurumsal düzeyde, parola yönergelerinin kullanıcı etrafında odaklanması gerektiğini önermektedir. Yönergeler, kullanıcıların günlük işlerindeki benzersiz gereksinimlerini ve becerilerini yansıtmalıdır. Kuruluşlar, insan-bilgisayar etkileşimi ilkelerine uyarak ve özel kullanımı hesaba katarak parola yönetiminde kullanıcı etkinliğini ve verimliliğini artırırken güvenliği en üst düzeye çıkarabilir. Ayrıca, işletmeler Telepathwords gibi yeni parola teknikleri ve cihazları kullanarak sıkı parola oluşturma standartlarını analiz etmeye ve uygulamaya çalışmalıdır. Buna ek olarak, işletmeler çalışanlarının zayıf ya da etki altında kalmış şifreler kullanmalarını önleyici bir çaba içinde olduklarından emin olmalıdır. Bu teknikler aracılığıyla şemayı aşmak, güvenliği büyük ölçüde artıracaktır (Blocki & Liu, 2023).

İki Faktörlü Kimlik Doğrulama ile Hayati Öneme Sahip Altyapının Korunması

İki Faktörlü Kimlik Doğrulama (2FA), kullanıcıların kullanıcı onayı için ikincil bir bileşen sağlamasını gerektiren bir güvenlik önlemidir. Bu yöntem, parola kimlik doğrulama sistemine bir kimlik doğrulama faktörü ekler. Bir değerlendirme platformunun 2FA uygulaması ile sahip olacağı bazı avantajlar vardır (Tellini & Vargas, 2017):

- **Yetkisiz erişim olasılığını ortadan kaldırır**: 2FA sadece bir kullanıcı adı ve şifre kullanmanın ötesine geçer. Kimlik doğrulama için tamamen ayrı bir sistem kullanır.
- **Şifre Hırsızlığına Karşı Koruma:** Kullanıcı adları ve şifreler her gün çalınmaktadır. 2FA ile, bir saldırganın gayrimeşru erişim elde etmek için yalnızca kullanıcının adı ve parola kimlik bilgilerinden daha fazlasına ihtiyacı olacaktır.

- **Azalan Yetkisiz Erişim Riski**: 2FA ile, bilgisayar korsanının hesaba erişimi tamamlamak için ihtiyaç duyacağı ekstra kimlik doğrulama katmanı nedeniyle yetkisiz veya kanıtlanmamış erişim olasılığı daha düşüktür ve kullanıcının telefonuna veya telefonunda oluşturulan bir koda sahip olması gerekir.
- **Artan Kullanıcı Güveni:** Kullanıcılar hesaplarının bir paroladan daha fazlasıyla korunduğunu bildiklerinde platforma olan güven ve inanç artabilir.
- **Güvenlik Standartları ile Uyumluluk:** 2FA kullanmak, oturum açma işlemlerinizi çevrimiçi güvenlik için en iyi uygulamalarla uyumlu hale getirebilir ve sektörünüzdeki belirli düzenlemeler veya standartlar tarafından gerekli kılınabilir.
- **Yaygın Parola Sorunlarının Azaltılması:** 2FA, kötü parola seçimleri ve yeniden kullanım gibi yaygın parola sorunlarının azaltılmasına yardımcı olur. Tek bir parolaya olan bağımlılığımızı azaltarak 2FA daha karmaşık parolalar kullanmamıza yardımcı olabilir.

2FA, son kullanıcıya erişim izni vermeden önce kullanıcıların iki farklı türde kimlik doğrulama faktörü sağlamasını gerektiren iki aşamalı bir doğrulama sürecidir. Üç tür faktör, kullanıcının bildiği bir şey (bilgi faktörü), kullanıcının sahip olduğu bir şey (sahiplik faktörü) ve kullanıcının olduğu bir şeydir (içkinlik faktörü).(De Cristofaro, Du, Freudiger, & Norcie, 2013). İki Faktörlü Kimlik Doğrulama yöntemi, parola merkezli kimlik doğrulama tekniklerini daha güvenli hale getirir. Hizmetler, riskleri ve faydaları ölçerek kullanıcı kimlik doğrulamasının güvencesini büyük ölçüde artırmak için dinamik faktör kombinasyonlarını kullanabilir (Han, Sun, Shen, Chang ve Shen, 2013).

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

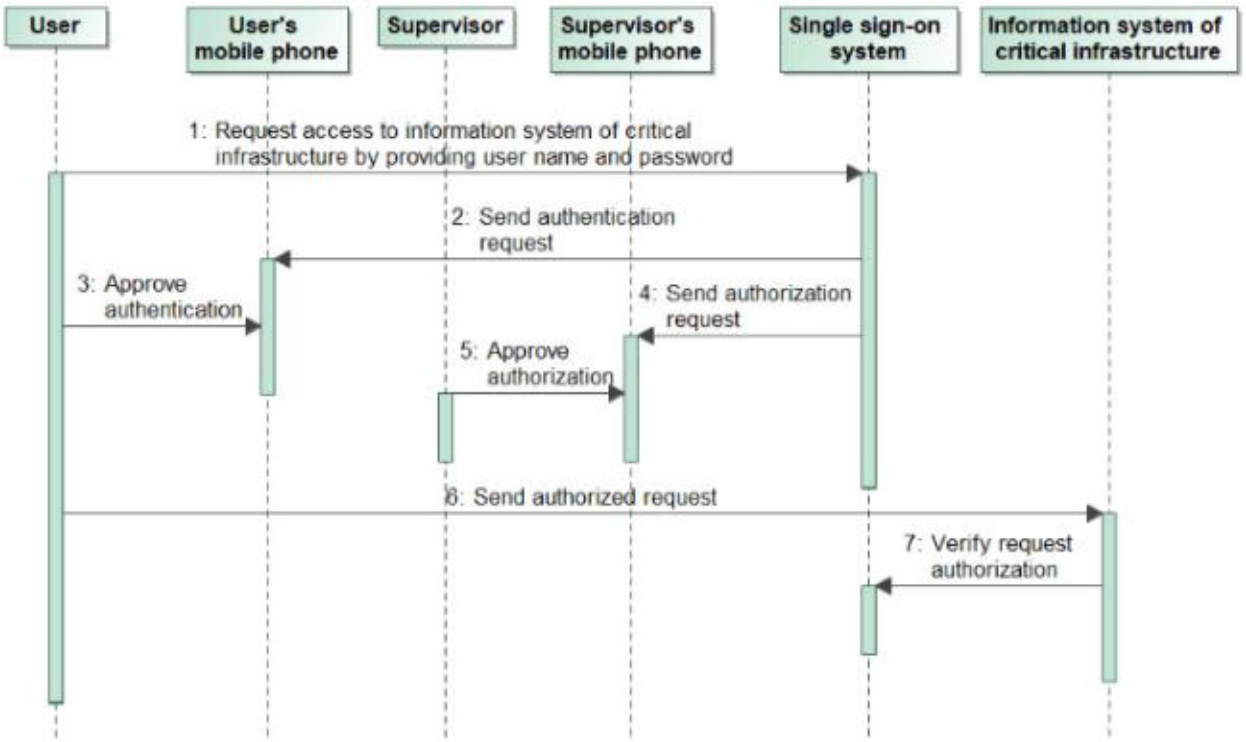
Tablo 1: Bazı kimlik doğrulama faktörleri sınıfları

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

(Bruzgiene & Jurgilas, 2019) kritik altyapı bilgi sistemlerine uzaktan erişimi güvence altına almak için üç adımlı bir süreçte çalışan bir kimlik doğrulama yöntemi sağlar. İlk olarak, kullanıcı hesap kimliğini ve şifresini girer. Doğru bilgiler girildikten sonra yerel güvenlik yetkilisinden (LSA) kullanıcının mobil cihazına bir kimlik doğrulama talebi gönderilir. Daha sonra kullanıcı telefonun ekranına tek bir dokunuşla talebi onaylamalıdır; bu, mobil cihazın uzak sistem için erişim haklarının seviyesini belirlemek üzere kullanıcının amir(ler)ine bir

yetkilendirme talebi göndermesini sağlayacaktır. Kullanıcı talebi amir(ler) tarafından başarıyla onaylandıktan sonra, talepte bulunan kullanıcıya uzak sisteme erişim hakları verilir

Şekil 1: Önerilen kimlik doğrulama yöntemi (Bruzgiene & Jurgilas, 2019)



Kaynak : (Bruzgiene & Jurgilas, 2019)

Zamanında Yazılım Güncellemeleri: Sistem Güvenliğini Güçlendirme

Yazılım güncellemeleri çok önemlidir çünkü hataları düzeltir veya sürücüler ve işletim sistemleri gibi yazılımların performansını artırır (Mathur, Malkin, Harbach, Péer ve Egelman, 2018). Yazılımı güncelleyerek, diğer yazılım ve donanım sistemleriyle uyumlu olmasını sağlar ve yazılımın en son sürümünü çalıştırarak sistemlerinizi güvende ve emniyette tutarsınız. Güncellemeler, bir bilgisayarı kötü amaçlı yazılımlardan ve güvenlik açıklarından korumak için gerekli olan güvenlik güncellemelerini, küçük hata düzeltmelerinden önemli iş akışı değişikliklerine kadar her şeyi içerebildikleri için önem derecesine göre değişen özellik güncellemelerini ve en son güncellemeye ulaşmadan önce önceki tüm güncellemelerin yüklenmesini gerektiren kümülatif güncellemeyi kapsar (Vaniea, Rader ve Wash, 2014). Bu iyileştirmeler, yazılım sistemlerinin güvenliğini ve işlevselliğini korumaya yardımcı olur. Gerekli tüm güncellemeleri aldığınızdan emin olmanız bu nedenle önemlidir.

Ancak, birçok kullanıcı algılanan faktörler nedeniyle yazılımlarını güncellemekten kaçınma eğilimindedir. Bu faktörler arasında kurulum süresi, yeniden başlatma *gerekliliği* ve kullanılan disk alanı gibi *güncelleme maliyetleri*; kullanıcının mevcut sistemden memnuniyeti, güncelleme nedenlerinin açıklığı ve güncellemenin kullanıcı tarafından algılanan önemi gibi *güncelleme gerekliliği* ve güncellemeler sırasında veri kaybına ilişkin endişeleri içeren *güncelleme riski* ve herhangi bir güncellemenin sistemi savunmasız hale getirebilecek bazı virüs veya kötü amaçlı yazılımlar taşıyabileceği yer almaktadır. (Mathur, Malkin, Harbach, Péer ve Egelman, 2018). Yazılımı yükseltmeyi ihmal etmek, bilgisayar sistemlerini, bilgisayarlara yeni virüsler ve solucanlar bulaştırmaya çalışabilecek bilgisayar korsanlarının eylemlerine açık hale getirebilir. Ayrıca bilgisayarlarınız için ciddi sonuçlar doğurabilir. Yamanmamış güvenlik açıkları sistemi daha az güvenli hale getirmekle kalmaz, aynı zamanda çoğu virüsün bu kadar başarılı olmasının da nedenidir.

Yazılım güncelleme teslim politikası, güvenlikle ilgili yazılım güncellemelerini değerlendirmek ve teslim etmek için zaman çizelgelerini ve yöntemleri tanımlayan kuruluşlar tarafından geliştirilen bir politikadır. Bu politika, kısıtlama izin veriyorsa, güvenlik açığı penceresini en aza indirmek için kısıtlı bir zaman aralığında (kısıtlama) güvenlik güncellemelerinin derhal teslim edilmesine odaklanır. Kuruluşlar kaynak kısıtlamalarına bağlı olarak daha stratejik bir yaklaşım benimseyebilir. Yenilikçi çözümler arasında, örneğin, güvenlik güncellemelerinin geniş son kullanıcı ağlarına son derece verimli ve uygun bir şekilde dağıtılmasını sağlamak için eşler arası Blok Zinciri tabanlı sistemler ve büyük ölçekli kaplama ağları yer alabilir. (Mugarza, Flores ve Montero, 2020). Politika, farklı seviyelerdeki güncellemelerin dağıtımdan önce ihtiyaç, maliyet ve ilişkili riskler doğrultusunda değerlendirilmesini sağlamak için farklı yama kategorilerini ve bunlarla ilişkili değerlendirme ve teslimat zaman çizelgelerini ayırmaktır.

İşte iş dünyası için yazılım güncelleme önerileri[1] :

- **Zamanında Yükleme:** Güvenlik güncellemelerinin zamanında yüklenmesi, sistemlerinizi güvenlik açıklarından ve tehditlerden korumaya yardımcı olabilir.
- **Açık İletişim:** Kullanıcılar güncellemelere neden ihtiyaç duyduğunuzu anlamadıkları için genellikle direnç gösterirler. Güncellemenin neden önemli olduğunu ve bunun sadece satıcı tarafından sağlanan rastgele bir yama olmadığını anlatmak önemlidir. E-postanızda bazı güncellemelerin halihazırda istismar edilmiş olabilecek güvenlik açıklarına yönelik yamalar olduğunu belirtmeniz de faydalı olacaktır
- **Kesintiyi En Aza İndirin:** Güncellemelerin uygulanmasını kolaylaştıracak şekilde sisteme sessiz kurulumları veya yapılandırmaları etkinleştirin. Kesintiyi en aza indirmenin bir başka yolu da güncellemeleri yoğun olmayan saatlerde dağıtmak ve dağıtmaktır.
- **Kullanıcı Eğitimi:** Proaktif güncelleme davranışını teşvik etmek için son kullanıcıları sistem güvenliğini ve işlevselliğini sürdürmede yazılım güncellemelerinin önemi konusunda eğitin

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

- **Test Prosedürleri:** Güncellemelerin dağıtımdan önce uyumluluk ve potansiyel riskler açısından titizlikle test edilmesini sağlamak için test prosedürlerini iyileştirin.
- **Güncellemeleri Farklılaştırın:** Güvenlik güncellemelerini özellik güncellemelerinden ayırın, böylece kullanıcılar her bir güncelleme türünün değerini anlar ve buna göre önceliklendirir.
- **Kümülatif Güncellemeler:** Kümülatif güncellemelerin etkilerini göz önünde bulundurun ve kullanıcıyı kritik güvenlik yamalarını yüklemeye teşvik edin.

Antivirüs Koruması: Sistem Bütünlüğünün Korunması

Göre (Rohith & Kaur, 2021)Anti-virüs yazılımı, değerli kişisel verilerin çalınmasını önlemek için işletim sistemini virüslerden, casus yazılımlardan, hacker saldırılarından ve diğer yetkisiz bilgisayar erişimlerinden koruyan özel bir programdır veya bilgisayarın yetkisiz kontrolü başka bir bilgisayar uygulamasıdır (ücretsiz, paylaşılan yazılım ve ticari). Anti-virüs yazılımı, bilgisayar dosyalarını, uygulama programlarını ve bilgisayarın işletim sistemlerini etkileyebilecek bilgisayar virüslerini tespit etmek için kullanılır. Bu nedenle, bilinen herhangi bir virüs imzasını tespit etmek ve böylece bilgisayar sisteminin ve dosyalarının olası bulaşmasını önlemek için bilgisayarın dosyaları ve belleği üzerinde düzenli incelemeler yapmak üzere de ayarlanabilir. Yeni virüsler ve varyasyonları düzenli olarak ortaya çıkmaya devam ettiğinden, anti-virüs yazılımını en son tanımlar ve virüs imzalarıyla düzenli olarak güncellemek önemlidir. En son virüs tehditlerini tespit ederek, anti-virüs yazılımının güncellenmesi, çalışırken bilgisayar tehditlerinin sürekli evrimine karşı sağlam bir savunma sağlar (Naie & Teymournejad, 2012).

Bilgisayarınızda bilgisayar virüslerinin varlığıyla ilişkili çeşitli belirtiler vardır ve bunlardan birkaçı aşağıda ayrıntılı olarak açıklanmıştır. Bu belirtilerin her biri bir virüs sorununa işaret edebilir. Bu nedenle, sistemi mümkün olan en kısa sürede antivirüs yazılımı ile taramak çok önemlidir (Kumar, 2008):

- Daha yavaş bilgisayar
- Temel görevler daha uzun sürer
- Kilitlenmeler ve çökmeler
- Sürekli disk etkinliği
- Aşırı CPU kullanımı
- İnternette gezinme eskisinden çok daha yavaş.
- Uygulamalar başlamıyor.
- Yetişkinlere yönelik içerik içeren açılır pencereler ve davetsiz mesajlar.
- Sabit diskler kalem numaraları.
- CD-ROM sürücüsü açılıyor ve kapanıyor.

Beklenmedik bir şekilde bu durumlardan bir veya birkaçıyla karşılaşırsanız, BT yöneticinizle iletişime geçin veya gerekli virüs kontrollerini gerçekleştirin. En iyisi olmasa bile tüm sistemlerde bir antivirüsün yüklü olmasının çok önemli olduğunu unutmamak gerekir. Bu, bir sistemin güvenliğini tehlikeye atmaya çalışan saldırganlar için daha yüksek bir zorluk seviyesi sağlamaya yardımcı olur (Min & Varadharajan, 2015).

İlerliyoruz, (Ncube & Maiden, 2004) bir kuruluş için antivirüs yazılımı seçimi sırasında karşılaşılan zorluklar ve araştırılması gereken hususlar hakkında değerli bilgiler sunmaktadır:

1. Diğer bilgi edinme teknikleriyle birlikte bir anket kullanın

2. Soruların kısa ve tedarikçilerden iyi yanıtlar almaya yönelik olduğundan emin olun.

3. Ürün açıklamasını gerçek ürünle daha iyi eşleştirebilmemiz için anket yanıtlarıyla birlikte belge isteyin.

4. Üründe ne söylediğinizi ve ne kadarını test edeceğinizi açıkça tanımlamanız test senaryosunu daha iyi tanımlamanıza yardımcı olacaktır.

5. COT yazılımını seçerken zamanla sınırlı olacağımızı anlayın ve farklı durumlarda daha hızlı olmak için süreç açıklama şablonlarını inceleyin.

6. Her şeyi test edemeyeceğinizi bilin. Bazı gereksinimlerin kısıtlamaları olabilir.

Veri Yedekleri: Kayıplara Karşı Bir Kalkan

Öngörülemese de, beklenmedik olaylar ve siber olaylar bir kuruluşun verilerine önemli miktarda zarar verebilir. İşte bu noktada veri yedeklemeleri devreye girer. Veri yedeklemeleri, siber güvenliğin ve güvenli bir dijital ortam sağlamanın kritik bir bileşenidir. Veri yedekleri, güvenlik ihlalleri durumunda kuruluşlar için harika bir araç olabilir. Verilerin kaybolmaya karşı korunmasının yanı sıra yedekleme sistemleri, dosyaların geçmiş sürümlerini geri yükleme olanağı sağlar, böylece dosya geçmişi korunur. Yedekleme araçlarının çoğu, aynı dosyanın birden fazla örneğini, her biri bir zaman damgasıyla ilişkilendirilmiş birçok formatta tutabilir. Ayrıca, sıkıştırma ve şifreleme neredeyse tüm yedekleme sistemlerinin ortak özellikleridir. Sıkıştırma, kullanıcıların dosyaları paylaşırken bir ağ veya İnternet üzerinden aktarmalarına yardımcı olur (Sampaio & Bernardino, 2015).

Veri yedekleme sistemlerinin teknikleri, tüm verilerin tam bir kopyasını oluşturan tam yedekleme, son tam yedeklemeden bu yana veri değişikliklerini depolayan diferansiyel yedekleme ve yalnızca bir önceki yedeklemenin alınmasından bu yana değişen veri bölümlerini kaydeden artımlı yedeklemeyi içerir. (Nadee & Somwang, 2021). Her yöntem, yedekleme işlemleri için farklı sonuçlar ve uygunluk sağlar. Güvenilir yedeklemeler dikkat çekicidir çünkü bazı veriler paha biçilmezdir ve ek verileri yeniden oluşturmak zaman/para kaybına neden olur (Traeger, Joukov, Sipek ve Zadok, 2006). Yedekleme verileri yalnızca veri kaybını önlemek için değil, aynı zamanda eski bir sürümü geri yüklemek için de kullanılır (Sampaio & Bernardino, 2015). Bu ikili işlevsellik hem veri kurtarma hem de belirli yasal standartlara uyumluluk açısından önemlidir. İşte küçük işletme yedeklemesi için bazı en iyi uygulamalar (Rock, 2023):

Veri Koruma Stratejisi: Küçük işletmelerin, BCP (İş Sürekliliği Planı) veya DRP'lerinin (Felaket Kurtarma Planı) bir parçası olacak ayrıntılı bir veri koruma planı tasarlamaları gerekir.

Yedekleme Çözümleri: İşletmeler basit yedekleme çözümleri kullanmamalı, bunun yerine minimum operasyonel kesintiyi garanti eden bazı sağlam BC/DR (İş Sürekliliği / Felaket Kurtarma) çözümleri seçmelidir.

Yedekleme Sıklığı ve Depolama: Düzenli yedekleme şarttır ve modern yedekleme çözümleri sık sık yedekleme yapar. Verileri hem yerinde hem de bulutta depolayan hibrit yedekleme korumasına sahip olunması önerilir.

Güvenlik ve Uyumluluk: Yedekleri Siber saldırılardan korumak ve ayrıca veri saklama politikalarına uymak önemlidir. Yedeklerin aktarım sırasında ve bekleme sırasında şifrelenmesi ek bir güvenlik olacaktır.

Verileri güvenli cihazlarda yedekleyin: Yedekleme cihazlarını yalnızca güvenli bir yerel alan ağı içinde giden iletişim için yapılandırın. Bu yaklaşım, bir siber suçlunun yedeklerinizin kontrolünü ele geçirmesini önlemeye yardımcı olacaktır.

Verileri ayrı cihazlarda yedekleyin: Yerel ağda fidye yazılımı oluştuğunda yedeklemelerin etkilenmesini önlemek için yedekleme cihazlarını yerel ağdan ayrı tuttuğunuzdan emin olun. Verileri buluta yedeklemenin avantajlarından biri, bunun ana kuruluş ofislerinden uzakta, bağlı herhangi bir yerden yapılabilmesidir.

Şifrelenmiş yedeklemeler kullanın: Kritik verileri yetkisiz erişime, tahrifata ve bozulmaya karşı korumak için şifreli depolama ve iletim kullanın.

Kurtarma yazılımı kullanarak tüm uç nokta verilerini yedekleyin: Veri kaybının çok önemli bir kaynağı kaybolan, çalınan veya bozulan dizüstü/masaüstü bilgisayarlardır. Sonuç olarak, kaybolan verileri yedekleyemez veya geri yükleyemezsiniz. Yedekleme cihazlarının masaüstü bilgisayarlar ve sunucular şeklinde olduğunu bilerek, her zaman herhangi bir bilgisayardaki tüm verileri korumak için kurtarma çözümlerini seçin ve uç nokta yedeklemesini buna göre seçin.

Kötü Amaçlı Kodlara Karşı Koruyucular: Anti-Malware Çözümlerini Anlamak

Kötü niyetli yürütülebilir dosyalar, bir bilgisayar sistemini istila etmek veya zarar vermek için oluşturulan ve bilgisayarın güvenliği için büyük bir tehlike oluşturan yetkisiz programlardır (Ye, Wang, Lİ ve Ye, 2007). Kullanıcılar genellikle farkında bile olmadan kötü amaçlı yazılımların kurbanı olurlar. Bir kullanıcının bilgisayarında bilgisi olmadan arka planda çalışan ve bilgi çalmak, cihazlarınızı temizleyecek virüsler veya dosyalarınızı silebilecek veya silmeyebilecek truva atları gibi şeyler yapan programdır. Casus yazılımlar, virüsler, solucanlar, Truva atları, fidye yazılımları ve reklam yazılımları kötü amaçlı yazılımların yaygın versiyonlarıdır. Her işletme sistemlerini günde birden fazla kez yedeklemeli ve sağlam bir kötü amaçlı yazılımdan koruma çözümü kullanmalıdır. Bir işletme için kötü amaçlı yazılımdan koruma yazılımı seçerken,

çözümün kuruluşun ihtiyaçlarına veya hedeflerine uygun olduğundan emin olmak için çeşitli faktörlerin dikkate alınması gerekir (Alharbi, Alzahrani, Asseri ve Taramisi, 2020):

Güvenlik Özellikleri: Gerçek zamanlı erişim, güvenlik duvarı koruması ve izinsiz giriş tespiti, bir kötü amaçlı yazılımdan koruma programına dahil edilmesi gereken temel güvenlik özellikleridir. Bu özellikler etkili tehdit yönetimi ve gözden kaçan tehditlerin olmadığından emin olmak için hayati önem taşır.

Operasyonel Özellikler: Kötü amaçlı yazılımdan koruma yazılımının aramanız gereken operasyonel özellikleri arasında yazılımı kurmanın ve kullanmanın ne kadar kolay olduğu, yazılımın hangi yönetim yeteneklerine sahip olduğu ve mevcut sistemlerinizle nasıl entegre olacağı yer alır.

Verimlilik: Kötü amaçlı yazılımdan koruma yazılımının zararlı yazılımları bulma ve kaldırma konusundaki verimliliğini değerlendirin. 100'e varan yüksek algılama yüzdesine ve minimum yanlış pozitif yüzdesine sahip çözümleri arayın.

Ölçeklenebilirlik: İşletme büyüdükçe ihtiyaçlarına göre ölçeklenebilen bir çözüm seçin. Kötü amaçlı yazılımdan koruma yazılımı çözümünün kuruluşunuzun mevcut ihtiyaçlarını karşılayabildiğinden ve gelecekteki ihtiyaçları karşılayabildiğinden emin olun.

Satıcı İtibarını Kontrol Edin: İyi bir itibar, yazılım sektöründe nadir bulunan bir özelliktir, ancak herhangi bir yazılım satıcısının en değerli özelliklerinden biridir. Yüksek kaliteli güvenlik çözümleri konusunda uzun bir geçmişe sahip kötü amaçlı yazılımdan koruma satıcılarını arayın. Bağımsız test kuruluşları tarafından tanınmışlar mı?

Maliyet: Dikkate alınması gereken ilk şey, kötü amaçlı yazılımdan koruma yazılımının fiyatıdır. Farklı satıcılar yazılımlarını farklı fiyat noktalarında ve lisanslama seçeneklerinde sunar, bu nedenle bütçenize uygun olduğundan emin olun. Bazı kuruluşlar bunu önemli bir faktör olarak sınıflandırırken, diğerleri bunu çok önemli değil olarak sınıflandırabilir.

Destek ve Güncellemeler: Tedarikçinin destek ve güncelleme kayıtlarını değerlendirin. Sorun çıkması durumunda düzenli güncellemeler ve teknik destek sağlayan bir satıcı bulun.

Uyumluluk, bir kuruluşun listeden çıkarması gereken şeylerden biridir çünkü uyumluluk sorunları yaşıyorsanız hiçbir yazılım etkili olamaz. Uyumluluk sorunları, bir kuruluşun yazılımının etkisiz hale gelmesinin en büyük nedenlerinden biridir.

Ünite 2 - Startup Operasyonlarında Dijital Hijyen Nasıl Alışkanlık Haline Getirilir?

Bir start-up operasyonunun günlük operasyonlarında Siber Güvenlik ve Siber hijyen uygulamalarını bir kültür haline getirmek çok önemlidir. Siber hijyen uygulamaları kişisel hijyen ile aynıdır, kişisel ve şirket verilerini/bilgilerini güvende ve emniyette tutmak için takip edilmesi gereken protokolleri sağlar (Alkhaledi & Hawamdeh, 2023). Start-up'lar, fon eksiklikleri nedeniyle bir siber olayın yaratacağı aksilikleri göze alamazlar. İş üzerindeki etkileri sadece finansal etkiyle sınırlı olmayıp, müşteri güveninin kaybedilmesi, itibar kaybı ve potansiyel yasal sonuçları da içermektedir ki bu da bir start-up için başarılı bir şekilde ölçeklenmek veya zamanından önce başarısız olmak arasındaki fark anlamına gelebilir. Siber hijyen konusunu ele almak için çok şey yapılmış olmasına rağmen birçok kuruluş hala iyi bir siber hijyen davranışından yoksundur (Kalhoro, Rehman, Ponnusamy ve Shaikh, 2021).

İyi bir siber hijyen davranışı, siber tehditleri ve siber hijyen sorunlarının ele alınmasına yönelik günlük zorlukları azaltmak için gereklidir. Bu bölüm, yeni kurulan şirketlerin günlük bir dijital hijyen rutini oluşturmaları için günlük olarak belirlenen stratejilerin ana hatlarını çizmeye ve genişletmeye hizmet etmektedir.

2.1. Girişiminizin Dijital Sağlığını Değerlendirme

Siber güvenlik risk değerlendirmesi, iş planlamasının önemli bir parçasıdır; bir kuruluşun dijital varlıklarına ve operasyonlarına yönelik risklerin belirlenmesini, değerlendirilmesini ve tahmin edilmesini içerir. Uygulanan siber güvenlik risk değerlendirme yöntemi, kuruluşun güvenlik duruşlarını değerlendirmesini, bilgilerine ve sistemlerine değer atamasını, mevcut güvenlik altyapısının ve faaliyetlerinin etkinliğini tahmin etmesini ve ayrıca belirli risklerin gerçekleşmesi durumunda ortaya çıkacak hasarın büyüklüğünü tahmin etmesini sağlar. Kuruluşlar, belirlenen riskleri önceliklendirerek savunmalarını güçlendirmek ve iş sürekliliğini sağlamak için kaynakları etkin bir şekilde tahsis edebilirler.

Çok sayıda çalışma, bir işletmeye yardımcı olabilecek siber güvenlik risk değerlendirmesinin farklı yönlerine ilişkin değerli bulgular sunmaktadır. (Chavez, ve diğerleri, 2020) KOBİ'lerde dijital araçların kullanımıyla etkili sapma yönetiminin ana adımlarından biri olarak bilgi ihtiyaçlarının değerlendirilmesini de göstermektedir. Prosedürler için toplanması gereken bilgi türlerine ve verilerin kritiklik düzeyine karar vermek, dijital sistemlerin entegrasyon riskini en aza indirmeye yardımcı olacaktır. (Elmarady & Rahouma, 2021) havacılık siber güvenliğinde risk değerlendirme sürecini özetlemiştir, ancak bu uygulamalar KOBİ'lerde risk değerlendirmesinde genel bir çerçeve olarak kullanılabilir:

1. Korunması gereken sistemleri belirleyin. Sistemlerin ne yapmak üzere tanımlandığının anlaşılmasıyla, bu sistemlere yönelik potansiyel tehditlerin belirlenmesi kulağa basit gelmektedir.

- Sistemleri anlayarak potansiyel tehditleri tanıyın.

- Değerlendirilecek sistemlerin sınırlarını tanımlayın ve bunları açıklayın.

2. Sistemde kayba veya zarara neden olabilecek her şeyi listeleyin. Bir güvenlik hedefinin gerçekleştirilememesine doğrudan veya dolaylı olarak neyin neden olabileceğini ve bir tehdit ile bir güvenlik açığı arasındaki farkın ne olduğunu anlayın.

- Sisteme doğrudan veya dolaylı olarak zarar verebilecek senaryoları belirleyin.

- Sistemin bütünlüğünü, gizliliğini ve kullanılabilirliğini etkileyebilecek tehditleri değerlendirin.

3. Tehditlerin olasılığını ve etkisini değerlendirin. Bir tehdidin gerçekleştirilebileceği tohumun değerlendirilmesinde birçok faktör ele alınmalıdır.

- Tehditlerin olasılığını değerlendirin.

- Tehditlerin güvenlik, verimlilik, ekonomi, siyaset ve kamu güveni üzerindeki potansiyel etkisini değerlendirin.

4. Risk seviyelerini belirleyin. Risk seviyelerini değerlendirin.

- Olasılık, güvenlik açığı değerlendirmeleri ve tehdit etkisini kullanarak risk profilini analiz edin.

- Risk seviyelerini niteliksel terimlere dönüştürün ve risk tolere edilebilirliğini belirleyin.

- Standartlaştırılmış bir metodoloji kullanarak risk seviyelerini kategorize edin.

Riskleri kabul edilebilir seviyelere indirmek için gereken azaltma önlemlerini uygulayın. Kuruluşlar bu adımları izleyerek siber güvenlik risklerini etkili bir şekilde değerlendirebilir, tehditleri belirleyebilir ve kritik sistemleri korumak için politikalar uygulayabilir.

2.2. Dijital Hijyen Kültürünün Oluşturulması

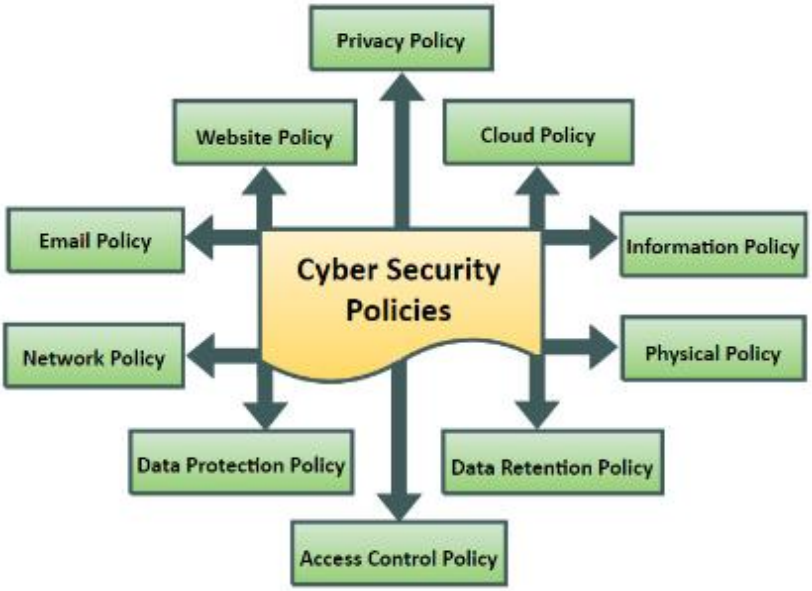
Dijital hijyen kültürü, gelişen bir dijital ekosistemin oluşturulması, ilk koşul olarak öncelikle kurum içine yerleştirilmelidir. Bu, yönetim tarafından yukarıdan aşağıya doğru yönlendirilmelidir. Sadece dijital refah hakkında konuşmak yeterli değildir, aynı zamanda üst yönetim tarafından uygulanmalıdır. Bu da politika geliştirmekle başlar. Liderler, veri yönetimini yöneten ve güvenliği artıran kapsamlı bir politikayı yönlendirmeli ve geliştirmelidir. Düzenli bir eğitim seansı son derece gereklidir. Çalışanlar arasında nasıl güvende kalınacağı ve Dijital Güvenliğin en son en iyi uygulamaları konusunda farkındalık yaratmak için düzenli bir program olarak alınmalıdır. Açık iletişim son derece kritiktir. Çalışanların rahatça iletişim kurabildikleri, endişelerini dile getirebildikleri ve ayrıca herhangi bir güvenlik sorununa neden olabilecek şüpheli bir şey bulduklarında bildirebildikleri bir kuruluşta şeffaf bir kültüre sahip olmak çok önemlidir. Ancak bu şekilde dijital hijyen ve güvenliği koruyacak bir kültürün oluşmasını sağlayabiliriz.

2.2.1. Politika geliştirme

Güçlü bir siber güvenlik politikasına sahip olmak, Küçük ve Orta Ölçekli İşletmelerin (KOBİ) dijital varlıklarını güvence altına almaları ve operasyonel sürekliliği sağlamaları için çok önemlidir. Araştırmalar, KOBİ'lerin bütçe yetersizliği, uzman eksikliği ve siber tehditlerdeki artış gibi çeşitli zorluklarla karşılaştığını göstermiştir (Neri, Niccolini ve Martino, 2023)Bu nedenle KOBİ'lerin siber farkındalıklarını ve hazırlık durumlarını iyileştirmeleri gerekmektedir. Siber güvenlik önlemlerinin alınması, yeterli bilgi işleme kapasitesine sahip güvenilir bir sistem oluşturmanın yanı sıra veri ihlallerini önemli ölçüde azaltabilir ve dahili süreç güvenliğini artırabilir (Hasani, O'Reilly, Dehghantanha, Rezania ve Levallet, 2023). Ayrıca, KOBİ'lerin siber saldırılara karşı dayanıklılığı, siber güvenlik politikaları aracılığıyla geliştirilebilir. siber dayanıklılığa yönelik bütüncül bir yaklaşımın uygulanması, KOBİ'lerin siber saldırıları öngörme, tespit etme, bunlara karşı koyma, bunlardan kurtulma ve siber saldırı sonrasında gelişme kabiliyetlerini artırabilir (Carias, Borges, Labaka, Arrizabalaga ve Hernantes, 2020).

İşletmeler siber güvenlik politikalarını tasarlarken farklı alanları göz önünde bulundurmalı ve ihtiyaçlarına göre uygun alanda siber güvenlik politikaları üretmelidir. Kurumlar, siber güvenlik politikalarını ve uygulamalarını ilerletmek için siber güvenlik politikaları taksonomisini geliştirmek için parçaları kullanabilirler. tarafından belirtilen siber güvenlik politikaları taksonomisinin bileşenleri (Mishra, Alzoubi, Gill ve Anwar, 2022) Şekil 2'de gösterilmiştir:

Şekil 2: Siber güvenlik politikaları taksonomisi

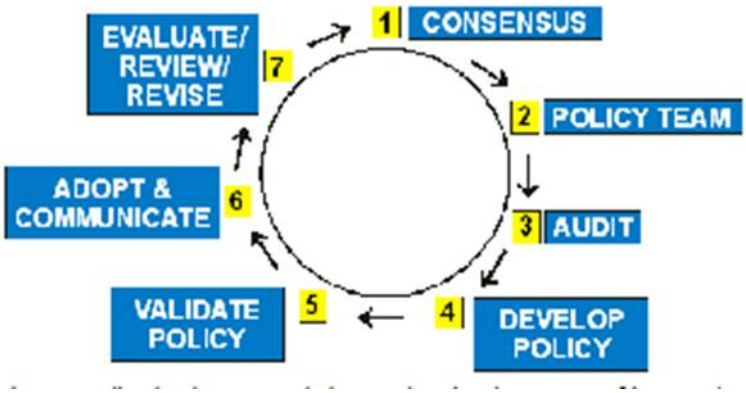


Kaynak: (Mishra, Alzoubi, Gill, & Anwar, 2022)

1. Gizlilik Politikası: Hassas kişisel verilerin korunmasına ve veri koruma düzenlemelerine uygunluğun sağlanmasına odaklanır.
2. Web Sitesi Güvenliği: Kullanıcı verilerini korumak için web sitelerini siber tehditlere ve güvenlik açıklarına karşı güvence altına almayı içerir.
3. Bulut Bilişim Güvenliği: Bulutta depolanan verileri korumak için bulut tabanlı hizmetlere yönelik güvenlik önlemlerini ele alır.
4. E-posta Güvenliği: E-posta iletişimlerinin güvenliğini sağlamaya ve e-posta tabanlı siber tehditleri önlemeye odaklanır.
5. Fiziksel Güvenlik: Yetkisiz erişimi önlemek için BT altyapısına ve kritik varlıklara fiziksel erişimin güvence altına alınmasını içerir.
6. Ağ Güvenliği: Bilgisayar ağlarını siber tehditlerden ve yetkisiz erişimden korumaya odaklanır.
7. Bilgi Güvenliği: Hassas bilgilerin korunmasına yönelik önlemleri kapsar
8. Erişim Kontrolü: Yetkisiz erişimi önlemek için sistemlere ve verilere kullanıcı erişimini yönetmeyi içerir.
9. Veri Saklama: Verilerin yaşam döngüsü boyunca saklanması ve yönetilmesine yönelik politikaları ele alır.
10. Veri Koruma: Şifreleme ve güvenlik kontrolleri aracılığıyla verilerin kaybolmaya, çalınmaya veya yetkisiz erişime karşı korunmasına odaklanır.

Eksiklikleri ve hedefleri öğrendikten sonra, siber güvenlik politikalarını bu alanları kapsayacak şekilde tasarlayabilirsiniz. Politika tasarımı için faydalı bir çerçeve şu şekilde özetlenmiştir (Lubua & Pretorius, 2019) Şekil 3'te gösterilmiştir. Politika Geliştirme Döngüsü, bir tür politika geliştirilmesini gerektirecek konuların farkına varılmasını, bir politika ekibi oluşturulmasını, paydaşlarla bir araya gelinmesini ve paydaşların toplanmasını, politikanın onaylanmasını, her değerli kararla birlikte politikanın benimsenmesini, politikanın üç yıl sonra ele alınmamasını, politikanızın geri bildirim ve değişiklikle azaltılmasını içerir. Süreç boyunca paydaş katılımının sağlanması, farklı insan gruplarından girdi alınması önemlidir. Politika ayrıca resmileştirilmeli, kurumsal hedeflerimizle ve yasa gereklilikleriyle uyumlu olduğundan emin olunmalıdır. Politikalar düzenli olarak gözden geçirilmeli ve güncelliğini yitirdiğinde güncellenmelidir. Düzenli gözden geçirmeler yapılmalı ve güncellemeler gerekli olmalıdır. Politikalar buna uygun olarak bir kuruluştaki veya belirli bir bağlamdaki çevresel değişiklikleri zorlayacak ve aynı zamanda işletecektir.

Şekil 3: Politika geliştirme döngüsü



Kaynak: (Lubua & Pretorius, 2019)

2.2.2. Düzenli eğitim

Çalışanların siber hijyen konusunda en iyi uygulamalar konusunda eğitilmesinde hayati önem taşıyan bir husus, davranışlarını ve bilgilerini etkileyen çok sayıda faktörün incelenmesidir. Yakın zamanda yapılan bir çalışmada (Cain, Edwards ve Still, 2018) kullanıcıların genellikle yapmaları gereken temel eylemlerin ve bunların etkilerinin farkında olmadıkları ve dolayısıyla davranışlarını etkiledikleri gerçeğine işaret etmektedir. Çoğu kullanıcı, ilgili risklerin farkında olmalarına rağmen en iyi güvenlik uygulamalarını takip etmenin tam olarak ne anlama geldiğini anlamaktan yoksundur. Önemli sayıda kullanıcı da risklerin farkında olabilir ancak yine de güvenlik kavramını daha iyi kavramak için uygun önlemleri alamayabilir. Tarafından yapılan bir başka çalışma (Neigel, Claypoole, Waldfogle, Acharya ve Hancock, 2020) siber ihlallere ve risklere katkıda bulunan insan faktörleri gibi faktörleri sunmaktadır. Kötü siber hijyen uygulamaları, farkındalık eksikliği, davranışsal önyargılar, eğitim boşlukları ve yetersiz eğitim, eğitim ve farkındalıkla ele alınabilecek insan faktörlerine önemli ölçüde katkıda bulunur ve güvenlik açığını büyük ölçüde azaltabilir ve böylece siber dayanıklılığı da artırabilir.

Çalışanlar için siber güvenlik eğitimi, kuruluşların bilgilerini korumak için proaktif bir yaklaşım benimseyebilmeleri açısından çok önemlidir. Çalışan eğitimi sadece çalışanları eğitmekle kalmaz, aynı zamanda tüm çalışanlarda var olan siber tehditlerin türü, bir siber suçlunun başarılı bir saldırısının sonuçlarının neler olabileceği ve bir kuruluşun istikrarını bozması durumunda buna nasıl karşı koyulacağı konusunda farkındalık yaratır. Kuruluşun tüm çalışanlarını siber güvenlik konusunda bilgili hale getirmek ve şirketin değerli varlıklarına yönelik herhangi bir tehdidi açıklamak için eğitmesi gerekir (Singh, Mohanty, Swagatika ve Kumar, 2020).

İşte siber siber güvenlik eğitimi için bazı en iyi uygulamalar (Mughal, 2019) :

- Düzenli Eğitim: Şirketin son kullanıcılarına, sorumlulukları dahilinde her zaman ortaya çıkan yeni tehditler hakkında bilgi sahibi olmaları ve güncel kalmaları için güvenlik eğitimi vermeye devam edin.
- Özel veya Uyarlanmış İçerik: Her zaman IoT cihazının riskine ve son kullanıcı rolü endişesine dayanan özel veya uyarlanmış eğitim içeriği kullanın.
- İnteraktif Öğrenme: Son kullanıcıların ilgisini neyin çektiğini ve öğrenme süreçlerini bilmek önemlidir; bu, kullanıcının ilgisini bu şekilde çekmeye devam etmek için atölye çalışmalarını etkileşime sokmaya ve simüle etmeye yardımcı olur.
- Açık İletişim: IoT güvenliği ve uygulamalarına dayalı sınırlamalarla ilgili politikayı her zaman en iyi şekilde iletin ve kullanıcı bunun farkında olsun.
- Pekiştirme ve Hatırlatmalar: Son kullanıcıya güvenlikle ilgili hatırlatmalarda bulunun ve son kullanıcıların farkındalığını her zaman sağlamaya devam edin.
- Teşvikler ve Ödüller: Son kullanıcıları eğitimi tamamlamaya veya Olayları raporlamaya teşvik eden ödüller ve teşvikler yoluyla siber güvenliğin iyi uygulanmasını sağlayın ve teşvik edin.
- Değerlendirme ve Geri Bildirim: Kullanıcı davranışını ve herhangi bir katılım gösterilmişse program görevlisinin nasıl çalıştığını izleyin.

2.2.3. Örgütsel Kültür

Kültürel hazırlık kavramı kendi kuruluşunuzun siber güvenlik hazırlığına nasıl uygulanabilir? Araştırmalar, siber güvenlik konusunda güçlü bir kültüre sahip kuruluşların siber tehditlerle başa çıkmaya daha hazırlıklı olduğunu göstermiştir (Berlilana,Noparumpa, Ruangkanjanases, Hariguna ve Sarmini, 2021). Siber güvenlik kültürü, siber güvenlikle ilgili risk yönetimi çerçevelerini, yönetişimi, politikaları ve çalışan davranışlarını şekillendiren genel kurum kültürünün ayrılmaz bir unsurudur (AL-Nuaimi, 2024). Ayrıca kuruluşlar, güvenlik girişimlerini destekleyerek, etkili iletişim kurarak ve çalışanların aktif katılımını sağlayarak üst yönetim liderliğinden ve kurum kültüründen yararlanarak çalışanların bilgi güvenliği politikalarına uyumunu teşvik edebilir (Hu, Dinev, Hart ve Cooke, 2012). Ortak bir güvenlik kültürü, departman veya iş rolünden bağımsız olarak tüm çalışanların siber tehdit risklerini anlamasına yardımcı olur. Bu da söz konusu bilgi güvenliği risklerini azaltmaya yönelik stratejilerin daha iyi uyumlaştırılmasına yardımcı olur (Fritzvold, 2017).

Tornatzky ve Fleischer (1990) tarafından geliştirilen Teknoloji-Organizasyon-Çevre (TOE) çerçevesi, çeşitli Bilgi Sistemleri (IS) ve Bilgi Teknolojisi (IT) ürün ve hizmetlerinin kuruluşlar tarafından benimsenmesini incelemek için bir temel sağlayan kapsamlı bir çerçevedir (Gangwar, Date ve Ramaswamy, 2015). Bu çerçeve, yeniliğin sadece teknik yönünü değil, aynı zamanda bir teknolojinin benimsenmesini açıklamak ve incelemek için organizasyonel ve çevresel görünümü de temsil eder (Rahayu & Day, 2015). Sonuç olarak, TOE çerçevesi, kuruluşlarda yeniliklerin benimsenmesini etkileyen faktörlerin net bir genel resmini göstermek için bu üç boyutu kapsamaktadır. Buna göre (Hasan, Ali, Kurnia ve Thurasamy, 2021) TOE çerçevesine dayalı olarak kuruluşlarda siber güvenlik hazırlığını etkileyen temel faktörler şunlardır:

Teknolojik faktörler

Kurumsal BT Altyapısının olgunluğu, bir kurumun siber saldırılara karşı hazır olma durumunu artırmada önemli bir rol oynar. Uzmanlar, BT cihazları ve kullanıcı yazılım uygulamaları konusunda gerekli kaynaklara sahip olarak BT altyapısında olgunlaşmak, hazır olma durumunu artırabilir.

Organizasyonel faktörler

Siber güvenliğe üst yönetim desteği, örgütsel yapı ve örgüt kültürü siber saldırılara karşı hazırlıklı olmak için önemli faktörlerdir. Üst yönetim desteğinin siber güvenlik hazırlığı üzerinde pozitif yönde anlamlı bir etkisi vardır.

Çevresel faktörler

Satıcı/Ortak İlişkileri, hükümet düzenlemeleri ve endüstriyel politikalar, kurumun siber saldırılara karşı hazır olma durumunu artırmaya olumlu yönde yardımcı olan dış çevre koşullarıdır

Siber güvenlik kültürünün geliştirilmesi, kurum kültürünü, alt kültürleri ve çerçeveleri dikkate alan karmaşık bir süreçtir. Kurum kültürü, güvenlik kültürlerinin şekillendirilmesinde önemli bir faktör olarak tanımlanmış

ve güvenlik kültürü de kurum içinde bir alt kültür olarak tanımlanmıştır. Kurumun bir parçası olan bir güvenlik kültürü oluşturmak için kurum, kültürü eserler ve önerilen değerler, paylaşılan varsayımlar, kurumsal bilgi ve gerekli operasyonel uygulamalar gibi boyutlar aracılığıyla keşfedebilir (Uchendu, Nurse, Bada ve Furnell, 2021).

Ünite 1 ve Ünite 2'yi Bir Araya Getirelim: Daha İyi Dijital Hijyen için Günlük Alışkanlıklar

Sürekli gelişen start-up ekosisteminde sağlam bir dijital hijyen kültürü şarttır. Yönetim tarafından yukarıdan aşağıya doğru yönlendirilen bu kültür, siber güvenlik ve veri korumanın önemini vurgular. Bu kültürün geliştirilmesine yardımcı olmak için start-up'lar, verilerin hem yerinde hem de bulutta depolandığı hibrit korumalı düzenli yedeklemeler uygulamalıdır. Bu, siber saldırılara ve sistem arızalarına karşı korunmaya yardımcı olacak ve verilerin her zaman güvende olmasını sağlayacaktır. Şifrelenmiş yedeklemeler de özellikle veri koruma uyumluluğunun tartışılmaz olduğu sağlık gibi sektörler için büyük önem taşımaktadır.

Sistemleri kötü amaçlı yazılımların bulaşmasından korumak için gerçek zamanlı tarama, davranış izleme, e-posta koruması ve web filtreleme gibi kapsamlı bir özellik paketi sunan kötü amaçlı yazılımdan koruma yazılımı kullanmak çok önemlidir. Öte yandan, start-up'lar olası tehditleri belirlemek, bunların olasılıklarını, etkilerini ve risk seviyelerini değerlendirmek için düzenli olarak proaktif siber güvenlik risk değerlendirmeleri yapmalıdır. Değerlendirmeler, kritik sistemleri korumak için etkili hafifletme önlemlerinin uygulanmasına rehberlik edecektir.

Verilerin güvenli bir şekilde ele alınmasını sağlamak için kapsamlı veri yönetimi politikaları ve protokolleri geliştirmek bir önceliktir. Politikalar, veri koruma, güvenli iletişim ve iyi Dijital Hijyen konularında en iyi uygulamalara yönelik politika ve prosedürleri tanımlamalıdır. Çalışanlar için düzenli eğitim Personelin dijital tehditler ve bunları önlemeye yardımcı olmak için neler yapabilecekleri konusunda daha iyi bilgilendirilmesi gerekir. Bu, personelinizin en son Tehditler ve Güvenlik önlemleri konusunda güncel kalmasını sağlayacaktır.

Çalışanların güvenlik endişelerini rahatça dile getirmelerine, şüpheli faaliyetleri bildirmelerine ve potansiyel tehditleri tartışmalarına olanak tanıyan kurumsal olarak açık iletişim, ortamın güvenliğini sağlamak için hayati önem taşır. Güçlü parolalar oluşturmak, yazılım yamalarını takip etmek, verileri şifrelemek ve güvenli iletişim kanalları kullanmak gibi günlük iyi siber hijyen uygulamalarına sahip olmak çalışanlar için bir alışkanlık haline gelmelidir.

Dikkate alınması gereken bir diğer maliyet-etkin unsur da farklı kötü amaçlı yazılımdan koruma çözümlerine, maliyete, desteğe, güncellemelere ve bütçenizle ve çalışma şeklinizle uyumluluğa bakmaktır. Startup'ların yukarıdaki unsurları eklenti olarak görmemesi gerektiği gibi, startup'lar da bu unsurları eklenti olarak görmemelidir. Startup'ların çevrimiçi ortamda güvende olmaları, varlıklarını korumaları ve müşterileri ve ortakları nezdinde güven tesis etmeleri gerekir; bunun için de startup'ların dijital Hijyen ve Siber Güvenliği

DNA'larının bir parçası haline getirmeleri gerekir. Girişimlerin dijital bakım ve siber hijyeni günlük operasyonel faaliyetlerinin tamamına yaymaları, girişimlerin çevrimiçi güvenliğini artırmanın ve böylece onları siber dirençli hale getirmenin tek gerçek yoludur. Siber Hijyen, dişlerinizi fırçalamak ve güvenli dijital uygulamalardır; Siber Güvenlik ise dişlerinizi fırçalamanın yanı sıra bir Ağız Koruyucu'ya sahip olmaktır. Birine sahip olduğunuzda diğerine sahip olamazsınız, her ikisi de çok gereklidir.

Ünite 3 - Dijital Hijyen Entegrasyonu: Vaka Çalışması ve Startup'lardan 1 İyi Uygulama

En İyi Uygulamalar: Startup'lar için En İyi Dijital Hijyen Araçları

Bağlam: Bu dijital çağda, start-up'lar ve herhangi bir özel işletme operasyonel faaliyetleri için teknolojiye büyük ölçüde güveniyorsa, tüm dijital tehditlerden ve veri ihlallerinden korunmak için dijital hijyeni yerinde tutmak çok önemlidir. Her start-up, dijital varlıklarını korumalarına yardımcı olacak belirli dijital hijyen araçlarına sahip olmalıdır, böylece operasyonel faaliyetlerine herhangi bir kesinti olmadan devam edebilirler.

En İyi Dijital Hijyen Araçlarının Belirlenmesi: Startup'lar, siber güvenliğin çeşitli yönlerini ele almak için kendilerini bir dizi dijital hijyen aracıyla donatmalıdır. İşte çok sayıda insanın güvendiği işletme ve kuruluşlardan birkaç aracın listesi.

1. **Antivirüs Yazılımı**: Antivirüs yazılımı, belirli bir yazılımdaki virüsleri ve diğer kötü amaçlı yazılımları engelleyen ve ortadan kaldıran ve aynı zamanda verileri çevrimiçi tehditlerden koruyan bir kontrol sistemidir.
2. **Güvenlik Duvarları**: Bir başka ağ güvenlik sistemi, bir ağa yetkisiz erişimi önlemek için tasarlanmış İnternet güvenlik cihazları için olan güvenlik duvarlarıdır.
3. **Parola Yöneticileri**: Bunlar, tüm siteler için güçlü, benzersiz parolalar oluşturmaya ve sürdürmeye yardımcı olacaktır.
4. **Şifreleme Araçları**: Hassas verilerin yetkisiz kullanıcılar tarafından okunamamasını sağlamak için hem bekleyen hem de aktarım halindeki verileri şifreleyin.
5. **İki Faktörlü Kimlik Doğrulama (2FA):** Oturum açma işlemi sırasında ekstra güvenlik ekler.
6. **Sanal Özel Ağlar (VPN)**: Genel ağlar üzerinden gizliliği ve veri güvenliğini korumak için güvenli ve şifreli bağlantılar sağlar.
7. **Güvenli Bulut Depolama**: dosyalarınızı güvenli bir noktada yedekleyebileceğiniz bir yer sunar. Yalnızca belirli kişilerin erişmesine izin vererek.

Dijital Hijyen Araçlarının Etkinliğinin Test Edilmesi

Öncelikle, seçtiğimiz araçların faydalı olduğundan emin olmamız gerekir:

1. **Uyumluluk Kontrolü**: Seçilen araçların kuruluşun mevcut sistemleriyle uyumlu olduğundan ve ayrıca iş akışlarına müdahale etmeyeceğinden emin olun.
2. **Kullanılabilirlik Değerlendirmesi**: Araçları kullanarak görevleri yerine getirmemiz gerekir. Aracı kullanarak günlük görevleri yerine getirmede başarılı olmak için çok fazla zaman ve veri girişi tüketmemesi
3. **Güvenlik Denetimi**: Etkinliği test etmek için araçlar düzenli olarak çalıştırılacak ve en son siber tehdit türlerine karşı gerçekten güvenli olup olmadıkları fark edilecektir
4. **Eğitim ve Farkındalık**: Ekibin dijital hijyenin önemi ve araçların etik ve doğru kullanımı konusunda eğitilmesi.

Dijital Hijyen Kültürünün Oluşturulması

Bağlam Her girişimde bir siber hijyen kültürü oluşturmak teknolojinin kendisi kadar önemlidir. Siber güvenlik farkındalığı ve hazırlığı, her bir start-up'taki her çalışanın siber güvenliğin önemini ve bir tehdide karşı korunmadaki rollerini kabul ettiği bir ortamı teşvik etme fikridir.

İşletmenizde Dijital Hijyen Kültürü Oluşturma:

1. **Liderlik Örneği**: Doğrudan liderlerin örnek teşkil etmesi ve iyi bir dijital hijyene sahip olması gerekir.
2. **Düzenli Eğitim**: Yeni tehditler ortaya çıktıkça çalışanları eğitin.
3. **Açık Politikalar**: İyi bir dijital hijyen için açık ve iyi tanımlanmış şirket içi politikalara sahip olun.
4. **Açık İletişimi Teşvik Etmek:** Çalışanların dijital hijyen sorunlarını bildikleri veya gördükleri için ödüllendirildikleri bir kültür oluşturun.
5. **Uyumluluğun Ödüllendirilmesi**: Dijital hijyen konusunda temel çizgiyi aştığını gösteren çalışanları ödüllendirin.

Sonuçlar ve Etki Bir Startup için dijital hijyen kültürünün beklenen sonuçları:

- **Azaltılmış Siber Saldırı Riski**: İyi bilgilendirilmiş bir ekip ilk savunma hattıdır.
- **Gelişmiş Veri Koruması**: Uygun dijital hijyen ile sizin ve müşterilerinizin işlerini koruyun.
- **Mevzuata Uygunluk** Siber güvenlik düzenlemelerine uyun ve mali ve diğer cezalardan kaçının.

Anahtar Çıkarımlar: Start-up'lar uzun vadede başarılı olmak istiyorlarsa temel bilgileri doğru bir şekilde öğrenmelidirler. En iyi dijital hijyen araçlarını kullanmak ve siber esneklik kültürünü işletmeye yerleştirmek, bir ihlalin uzun vadeli maliyetlerini azaltmak ve en kötüsü gerçekleşirse iyileşme süresini hızlandırmak için çok önemlidir.

Örnek Olay İncelemesi: SecureTech Startup - Siber Güvenlik için Dijital Hijyeni Benimsiyor

Yönetici Özeti: SecureTech, şirketlerini güvence altına almanın bir parçası olarak dijital hijyenin önemini fark eden bir fintech girişimidir. Bu vaka çalışması, saldırganların dijital alanlarına girmeleri için daha da

büyük bir boşluk yaratmak amacıyla kuruluşlarında yaptıkları farklı araçların ve kültürel değişimlerin ana hatlarını sağlayacaktır.

Giriş: Siber tehditlerin hızla geliştiği bir çağda, SecureTech'in dijital varlıklarını ve müşteri verilerini korumak için yapması gereken çok zor bir görevi vardır. Kuruluşun ilk aşamalarında şirket yönetimi, sağlam dijital hijyenin kendileri için sadece bir gereklilik değil, aynı zamanda çok kritik bir rekabet avantajı olduğu gerçeğini anlamıştır.

Durum Analizi: İlk siber güvenlik değerlendirmesinin ardından şirket, iyileştirilmesi gereken pek çok alan olduğunu keşfetti. SecureTech, dijital hijyen ve genel çalışan siber güvenlik farkındalığı ile ilgili olarak kullanılacak araçları geliştirdi.

Dijital Hijyen Araçlarının Belirlenmesi: Dijital Hijyen ile ilgili çok sayıda aracı değerlendirdikten sonra SecureTech, kendi özel durumlarına hitap edecek bir paket belirledi.

1. **BitDefender**: Tüm cihazlarınızı çeşitli tehditlere karşı korur.
2. **Cisco Güvenlik Duvarları**: Ağ trafiğini izler ve kontrol eder.
3. **LastPass**: Tercih edilen Parola Yöneticisi.
4. **VeraCrypt**: Tüm verilerinizi şifreler.
5. **Duo Güvenlik**: İki faktörlü kimlik doğrulama için kullanılır.
6. **NordVPN**: Uzaktan bağlantınızı ve işinizi meraklı gözlerden korur.
7. **Dropbox Business**: Yedeklerinizi ve dosyalarınızı bulutta güvenli bir şekilde depolar.

Dijital Hijyen Kültürünün Oluşturulması: SecureTech liderliği, şirket için bir dijital hijyen programı tasarladı ve uygulamaya koydu.

CEO Taahhüdü: Programın şirket genelinde kullanılmasına yönelik destek, CEO'nun onay damgasını vurmasıyla desteklendi.

1. **Aylık siber güvenlik eğitimi**: Ekibi en son tehditler ve trendler hakkında bilgilendirmek için atölye çalışmaları düzenlendi.
2. **Dijital Hijyen El Kitabı:** Kapsamlı bir dizi politika ve süreç, tüm çalışanlara Masaüstü Drop olarak sağlanmıştır.
3. **Güvenlik Şampiyonları:** Seçilen çalışanlar, kendi departmanları için Siber Güvenlik Savunucuları olmak üzere eğitilmiştir.

4. Güvenli Alışkanlıklar için Ödüllendirme ve Tanıma: Mükemmel dijital hijyene sahip bireyler tanınmış ve ödüllendirilmiştir.

Zorluklar ve Çözümler: Değişimimize yönelik itirazlar: yeni araçların benimsenmesi, dijital hijyen uygulamalarımızda kültürel değişim.

1. Engellerin Azaltılması: Yeni dijital araç setlerimizin her bir ekibimizin verimliliğini yavaşlatmak yerine artırdığından emin olduk.

2. Güvenlik Eğitimini Eğlenceli Hale Getirmek: Ekipleri siber becerilerine göre sıralayacak oyun tabanlı bir güvenlik eğitim programı uygulandı.

3. **Birliklerimizi Bilgilendirmek:** TeamSecureTech'in kaydettiği ilerleme ve dijital hijyen çabalarının şirketlerinin güvenliği üzerindeki ETKİSİ sürekli olarak iletildi.

Sonuçlar: Bir yıl içinde SecureTech raporladı:

• **100 Dijital Hijyen Aracının Benimsenmesi -** Seçilen araçlar personel tarafından tamamen benimsenmiştir

- Kimlik Avı Girişimlerinde %80 Azalma - Personel farkındalığının artması, şüpheli e-postaların daha hızlı fark edilmesini ve raporlanmasını sağladı

- İyileştirilmiş Uyumluluk Duruşu - Tüm düzenleyici standartlar karşılandı ve herhangi bir para cezasıyla karşılaşılmadı

Sonuç: SecureTech'in dijital hijyen konusundaki son derece proaktif tutumu, siber güvenliğini büyük ölçüde iyileştirmiş ve bir ihtiyat ve sorumluluk kültürü geliştirmiştir. Bu vaka çalışması, bir şirketin kültüründeki dönüşümle birlikte çalışan etkili bir kontrol çerçevesi aracılığıyla karmaşık bir tehdit ortamının nasıl alt edilebileceğini göstermektedir.

Çıkarımlar:

Doğru aracın seçilmesi çok önemlidir: startup'ların kendi özel ihtiyaçlarına ve iş akışlarına uygun dijital hijyen araçlarını aramaları gerekir

Kültür uyumu yönlendirir: güçlü bir dijital hijyen kültürü oluşturmak siber güvenlik risklerini azaltabilir

Bu bir iyileştirme sürecidir: siber güvenlik bir durum değil, devam eden bir süreçtir, tek seferlik bir eylem değildir ve düzenli güncellemelere ve eğitimlere ihtiyaç duyar

Referanslar

Alharbi, B., Alzahrani, H., Asseri, A., & Taramisi, K. (2020). Kötü amaçlı yazılım önleme verimliliği değerlendirme çerçevesi. *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* (s. 1-4). IEEE.

Alkhaledi, R., & Hawamdeh, S. (2023). Elektronik sağlık kayıtları ve siber hijyen: Kuveyt'teki hekimlerin farkındalık, bilgi ve deneyimlerine ilişkin nitel bir çalışma. *Proceedings of the Association for Information Science and Technology, 60(1)*, s. 21-30.

AL-Nuaimi, M. N. (2024). Kurumlarda siber güvenliği etkileyen insani ve bağlamsal faktörler ve yükseköğretim kurumları için çıkarımlar: sistematik bir inceleme. *Global Knowledge, Memory and Communication, 73* ((1/2)), 1-23.

Berlilana,Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Kurumsal Güvenliğin Benimsenmesinin Bir Sonucu Olarak Kurumsal Fayda: Siber Güvenlik Hazırlığı ve Teknoloji Hazırlığının Rolü. *Sustainability, 13*(24), 13761.

Blocki, J., & Liu, P. (2023). Ampirik şifre veri kümelerinin titiz bir istatistiksel analizine doğru. *2023 IEEE Güvenlik ve Gizlilik Sempozyumu (SP)*, 606-625.

Bruzgiene, R., & Jurgilas, K. (2019). İki faktörlü kimlik doğrulama kullanarak kritik altyapı bilgi sistemlerine uzaktan erişimin güvence altına alınması. *Electronics, 10*(15), 1819.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). Siber hijyen davranışları ve bilgisi üzerine keşifsel bir çalışma. *Bilgi güvenliği ve uygulamaları dergisi, 42*, 36-45.

Carias, J. F., Borges, M. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). KOBİ'lerde siber dayanıklılığın operasyonel hale getirilmesine yönelik sistematik bir yaklaşım. *IEEE Access*, *8*, s. 174200-174221.

Chavez, Z., Hauge, J. B., Bellgran, M., Gullander, P., Johansson, M., Medbo, L., & Ström, M. (2020). KOBİ'lerde verimli sapma yönetimi için dijital araçlar ve bilgi ihtiyacı değerlendirmesi. *Advances in Transdisciplinary Engineering., 13*(SPS2020), 24 - 35.

De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2013). İki faktörlü kimlik doğrulamanın karşılaştırmalı kullanılabilirlik çalışması. *arXiv ön baskı, 1309,* 5344.

Di Tizio, G., Armellini, M., & Massacci, F. (2022). Yazılım güncelleme stratejileri: Gelişmiş kalıcı tehditlere karşı nicel bir değerlendirme. *IEEE Transactions on Software Engineering, 49*(3), 1359-1373.

Elmarady, A. A., & Rahouma, K. (2021). Havacılık siber güvenlik risk değerlendirmesinin geliştirilmesi ve uygulanması da dahil olmak üzere sivil havacılıkta siber güvenliğin incelenmesi. *IEEE Access, 9*, 143997-144016.

Fritzvold, E. (2017). Kurumlarda Siber Güvenlik. *(Yüksek lisans tezi, Stavanger Üniversitesi, Norveç)*.

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Bütünleşik bir TAM-TOE modeli kullanarak bulut bilişimin benimsenmesinin belirleyicilerini anlamak. *Journal of Enterprise Information Management, 28*(1), 107-130.

Han, W., Sun, C., Shen, C., Chang, L., & Shen, S. (2013). Sayısallaştırılmış risk ve faydaya dayalı kimlik doğrulama faktörlerinin dinamik kombinasyonu. *Security and Communication Networks, 7*(2), 385-396.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Kuruluşların siber güvenliğe hazır olma durumlarının ve bunun performans üzerindeki etkisinin değerlendirilmesi. *Bilgi Güvenliği ve Uygulamaları Dergisi, 58*, 102726.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Siber güvenliğin benimsenmesi ve örgütsel performans üzerindeki etkisinin değerlendirilmesi. *SN Business &Amp; Economics, 3*(5).

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Çalışanların bilgi güvenliği politikalarına uyumunu yönetmek: Üst yönetimin ve örgüt kültürünün kritik rolü. *Decision Sciences, 43*(4), 615-660.

Inglesant, P. G., & Sasse, M. A. (2010). Kullanılamaz parola politikalarının gerçek maliyeti: vahşi doğada parola kullanımı. *Bilgisayar sistemlerinde insan faktörleri üzerine Sigchi konferansı bildirileri*, (s. 383-392).

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

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Yazılım mühendisleri arasında siber hijyen davranışının temel faktörlerinin çıkarılması: sistematik bir literatür taraması. *IEEE Access*, *9*, s. 99339-99363.

Kato, K., & Klyuev, V. (2013). Güçlü parolalar: Pratik sorunlar. *2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems(IDAACS). 2*, s. 608-613. IEEE.

Keszthely, A. (2013). Şifreler hakkında. *Acta Polytechnica Hungarica*, 99-118.

Kumar, P. (2008). Bilgisayar virüsü önleme ve anti-virüs stratejisi. *Sahara Sanat ve Yönetim Akademisi Serisi*.

Lubua, E. W., & Pretorius, P. D. (2019). Kamu kuruluşlarında siber güvenlik politikası çerçevesi ve prosedürel uyum. *Uluslararası Endüstri Mühendisliği ve Operasyon Yönetimi Konferansı Bildirileri*, (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). Yeni bir anti-virüs parazit kötü amaçlı yazılımın tasarımı, uygulanması ve değerlendirilmesi. *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). Siber güvenlik girişimleri politikaları: Karşılaştırmalı bir çalışma. *Sensors, 22*(2), 538.

Mugarza, I., Flores, J. L., & Montero, J. L. (2020). Endüstriyel Nesnelerin İnterneti (IoT) çağında güvenlik sorunları ve yazılım güncelleme yönetimi. *Sensors, 20*(24), Sens*ör*.

Mughal, A. A. (2019). Nesnelerin İnterneti (IoT) Çağında Siber Güvenlik Hijyeni: En İyi Uygulamalar ve Zorluklar. *Applied Research in Artificial Intelligence and Cloud Computing, 2*(1), 1-31.

Nadee, P., & Somwang, P. (2021). Unison synchronize yaklaşımının verimli artımlı veri yedeklemesi. *Bulletin of Electrical Engineering and Informatics, 10*(5), 2707-2715.

Naie, H., & Teymournejad, K. (2012). TOPSIS yönteminin uygulanmasıyla dünyadaki en iyi anti-virüsün seçilmesi. *Yaşam Bilimleri Dergisi, 9*(4).

Ncube, C., & Maiden, N. (2004). Uluslararası bir banka için cots anti-virüs yazılımı seçimi: Çıkarılan bazı dersler. *Bildiriler 1. MPEC Çalıştayı*.

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Bütünsel siber hijyen eğitimi: İnsan faktörleri için muhasebe. *Computers & Security*(92), 101731.

Neri, M., Niccolini, F., & Martino, L. (2023). BİT sektöründe kurumsal siber güvenlik hazırlığı: niceliksel-niteliksel bir değerlendirme. *Information &Amp; Computer Security, 32*(1), 38-52.

Pearce, M., Zeadally, S., & Hunt, R. (2010). Kimlik doğrulama güven yönetiminin değerlendirilmesi ve iyileştirilmesi. *Bilgi Yönetimi ve Bilgisayar Güvenliği, 18*(2), 124-139.

Rahayu, R., & Day, J. (2015). Rahayu, R., & Day, J. (2015). Gelişmekte olan ülkelerdeki KOBİ'lerin e-ticareti benimsemesinin belirleyici faktörleri: Endonezya'dan kanıtlar. *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). Anti-virüs tarafından kullanılan kötü amaçlı yazılım algılama ve önleme teknikleri üzerine kapsamlı bir çalışma. *2021 2nd International Conference on Intelligent Engineering and Management (iciem)* (s. 429-434). IEEE.

Sampaio, D., & Bernardino, J. (2015). KOBİ'ler için açık kaynaklı yedekleme sistemleri. *New Contributions in Information Systems and Technologies*, 823-832.

Sampaio, D., & Bernardino, J. (2015). KOBİ'ler için açık kaynaklı yedekleme sistemleri. *New Contributions in Information Systems and Technologies: Cilt 1*, 823-832.

Singh, D., Mohanty, N. P., Swagatika, S., & Kumar, S. (2020). Siber hijyen: Siber uzayda siber güvenlik için anahtar kavram. *Test Mühendisliği ve Yönetimi*, 8145-8152.

Tellini, N., & Vargas, F. (2017). *İki Faktörlü Kimlik Doğrulama: Dijital bir değerlendirme platformu için iki faktörlü bir kimlik doğrulama yönteminin seçilmesi ve uygulanması*.

Traeger, A., Joukov, N., Sipek, J., & Zadok, E. (2006). Veri yedekleme için ücretsiz web depolama alanı kullanımı. *İkinci ACM Depolama Güvenliği ve Bekası Çalıştayı Bildirileri*.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Bir siber güvenlik kültürü geliştirmek: Mevcut uygulamalar ve gelecekteki ihtiyaçlar. *Computers & Security, 109*, 102387.

Vaniea, K. E., Rader, E., & Wash, R. (2014). Güncellemeler tarafından ihanete uğramak: olumsuz deneyimler gelecekteki güvenliği nasıl etkiler? *Bilgi işlem sistemlerinde insan faktörleri üzerine SIGCHI konferansı bildirileri*, (s. 2671-2674).

Ye, Y., Wang, D., Lİ, T., & Ye, D. (2007). IMDS: Akıllı kötü amaçlı yazılım tespit sistemi. *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*, (s. 1043-1047).

Modül 3 - Startup'larda Dijital Hijyen

Ünite 1 - Dijital Hijyenin Startup Büyümesi ve Güvenliğindeki Rolü

Fiziksel sağlığımızı korumak gibi, dijital hijyeni de sağlam tutmak çevrimiçi ortamda daha güvenli olmanın anahtarıdır. Dijital hijyen, hem kişisel çevrimiçi yaşamlarımızda hem de profesyonel faaliyetlerimizde hepimiz için bir rutine dönüşmelidir.

Start-up'lar olarak, şirket içi kuralları ve politikaları tanımlarken, tüm çalışanların uyması gereken dijital hijyen kurallarını ve en iyi uygulamaları da dahil etmelisiniz.

İş faaliyetlerimizin çoğu çevrimiçi dijital ortamlar kullanılarak gerçekleştiriliyor. Bu nedenle, olası risklerin farkında olmalı ve bunları azaltmak ve girişiminizde iyi bir dijital hijyen sağlamak için belirli politikalar uygulamalısınız.

Sadece kontrol etmeniz gereken resmi bir görev olan dijital hijyen politikasını uygulamayı düşünmeden önce, bunun getirebileceği tüm faydaları düşünün.

Bu nedenle, girişiminiz için bir dijital hijyen politikası uygulamak hoş değil, çalışanlarınızın profesyonel ve kişisel yaşamlarını korumak için olmazsa olmazdır. Girişimlerde dijital hijyen uygulamalarına duyulan ihtiyacı vurgulamak için bazı nedenlere ihtiyacınız varsa, dijital hijyenin onlar için neden çok önemli olduğunu gözden geçirelim.

Startup'lar, sınırlı kaynaklara sahip ve büyük kuruluşların güçlü güvenlik altyapısına sahip olmayan küçük kuruluşlardır. Bu durum onları siber suçlular için cazip hedefler haline getirir ve siber tehditlere karşı daha duyarlı kılar. Dijital hijyen politikası, etkili güvenlik önlemlerinin uygulanmasına ve olası risklerin azaltılmasına yardımcı olur.

Sonuç olarak, girişimler için dijital hijyen politikası güvenlik, güven oluşturma, ölçeklenebilirlik, maliyet etkinliği ve operasyonel verimlilik için temel bir unsur olarak hizmet eder. Günümüzün dijital iş ortamında girişimin sürdürülebilir başarısı ve büyümesi için çok önemli olan sorumlu ve güvenli dijital uygulamaların tonunu belirlemeye yardımcı olur.

Ünite 2 - Startup'larda Dijital Hijyen Uygulamalarını Hayata Geçirmenin Faydaları

İyi dijital hijyen uygulamalarını hayata geçirmenin faydaları nelerdir?

Basit bir ifadeyle, iyi bir dijital hijyen uygulamak, günümüzün teknoloji odaklı iş ortamında çevrimiçi varlığınızı güvenli ve sağlıklı hale getirir. Yani, faydalar iki düzeydedir:

1. **Güvenlik ve bakım**
2. **Sağlık**

Başlıca faydalarını öğrenelim!

1. **Güvenlik ve bakım**

İyi dijital hijyen politikaları ve en iyi uygulamaları uygulamak iş yerinizin (ve kişisel) dijital ortamını güvende tutacaktır. Bakım kurallarını tanımlamayı, tüm çalışanların iç politikadan haberdar olduğundan ve kuralların yeni olası tehditlerle güncel olduğundan emin olmayı unutmayın.

Ekibinizin olası yeni siber tehditlere doğru şekilde yanıt vermek için gerekli bilgiye sahip olduğundan emin olmak amacıyla periyodik siber güvenlik farkındalık eğitimleri gerçekleştirmeniz önerilir.

Dijital ortamda güvenliklerini korumak için iyi dijital hijyen uygulamalarını hayata geçiren ve sürdüren startup'lar için temel faydaları nasıl özetleyebiliriz?

- **Güvenlik ve veri gizliliği uyumluluğu**

Hassas bilgilerin korunması çok önemlidir. Yazılımların düzenli olarak güncellenmesi, güçlü parolaların kullanılması ve şifreleme tekniklerinin uygulanması hassas verilerin siber tehditlere karşı korunmasına yardımcı olabilir. İyi bir dijital hijyen, hassas bilgilerin korunmasına yardımcı olur ve yetkisiz erişimi önleyerek veri ihlali riskini azaltır. Veri koruma yönetmeliklerine uymak, girişimin yasal sorunlardan kaçınmasını ve müşterilerle güven oluşturmasını sağlar.

Ayrıca, finansal verilerin ve müşteri verilerinin korunması startup'lar için son derece önemlidir. Dijital hijyen, güvenli çevrimiçi işlemler ve finansal veri bütünlüğü sağlar.

- **İtibar yönetimi ve güven oluşturma**

Müşteriler ve iş ortakları dijital güvenliğe öncelik veren işletmelere güvenir. Dijital güvenlik ve gizliliğe bağlılık göstermek, girişimin itibarını artırabilir ve müşteriler, yatırımcılar ve iş ortakları nezdinde güven oluşturabilir. Ayrıca, güvenlik olaylarının olumsuz etkilerinden de kaçınılabilir. Kullanıcı dostu bir web sitesi ve güvenli çevrimiçi işlemler de dahil olmak üzere bakımlı dijital varlıklar profesyonel bir imaja katkıda bulunur.

- **Uyumluluk ve yasal koruma: mevzuat gerekliliklerinin karşılanması**

Birçok sektörde veri koruma ve gizlilikle ilgili katı düzenlemeler vardır. Sektöre özgü düzenlemelere ve uyumluluk standartlarına bağlı kalmak, girişimlerin yasal komplikasyonlardan, para cezalarından ve itibar kaybından kaçınmasına yardımcı olur. Bu düzenlemeleri benimsemek yalnızca start-up'ı yasal sonuçlardan korumakla kalmaz, aynı zamanda güvenilir bir marka imajı oluşturmaya da yardımcı olur.

Denetimler ve incelemeler de bir diğer önemli unsurdur. Dijital uygulamaların düzenli olarak denetlenmesi, girişimin gelişen yönetmelikler ve endüstri standartlarıyla uyumlu kalmasını sağlar.

- **Operasyonel süreklilik: kesinti süresinin azaltılması**

Kötü amaçlı yazılım saldırıları veya veri kaybı gibi siber güvenlik olayları önemli ölçüde kesintiye yol açabilir. Dijital hijyen önlemleri, bu tür olayların önlenmesine ve azaltılmasına yardımcı olarak iş operasyonlarının kesintisiz devam etmesini sağlar.

- **Maliyet Tasarrufu: mali kayıpların önlenmesi**

Bir siber güvenlik olayından kurtulmak pahalı olabilir. Düzenli yedeklemeler ve güvenli depolama yöntemleri, veri kaybını önleyerek girişimleri kayıp bilgilerin kurtarılmasıyla ilgili potansiyel olarak yüksek maliyetlerden kurtarabilir. Dijital güvenlik önlemlerine erkenden yatırım yapmak, fidye yazılımı veya veri ihlalleri gibi siber saldırılardan kaynaklanan potansiyel mali kayıpları önlemeye yardımcı olan proaktif bir yaklaşımdır.

- **İnovasyon ve büyüme: inovasyonu teşvik etmek**

Güvenli bir dijital ortam, girişimlerin siber güvenlik endişeleriyle sürekli olarak dikkatleri dağılmadan inovasyona odaklanmalarını sağlar. Bu, yaratıcılığı teşvik eder ve iş büyümesini hızlandırır. Rutin görevleri otomatikleştirerek ve dijital iş akışlarını optimize ederek startup'lar inovasyona ve stratejik girişimlere odaklanmak için zaman ve kaynak ayırabilir. İyi bir dijital hijyen, girişimin yeni araçları ve teknolojileri benimsemeye teknolojik olarak hazır olmasını ve pazarda rekabetçi kalmasını sağlar.

- **Müşteri güveni ve sadakati: müşteri bilgilerinin korunması**

Müşterilerin, kişisel bilgilerinin güvenliğine öncelik veren işletmelerle etkileşim kurma olasılığı daha yüksektir. Dijital hijyen, müşteri güveni ve sadakati oluşturarak uzun vadeli ilişkilere katkıda bulunur.

- **Tedarik zinciri güvenliği: satıcı ve iş ortağı güvenliğinin sağlanması**

İyi dijital hijyen uygulamaları, startup'ın dahili sistemlerinin ötesine geçerek satıcılar ve ortaklarla güvenli iletişim ve veri alışverişini de kapsar ve uçtan uca güvenli bir tedarik zinciri sağlar.

- **Ortaya çıkan tehditlere uyum sağlama: tehditlerin önüne geçmek**

Dijital hijyen, en son siber güvenlik tehditleri hakkında bilgi sahibi olmayı ve bunlara karşı önlemler almayı içerir. Bu uyarlanabilirlik, siber tehditlerin sürekli gelişen ortamında çok önemlidir.

2. **Sağlık**

Gün içinde zamanımızı geçirdiğimiz çok sayıda dijital teknoloji ve çevrimiçi platformdan bunalmış durumdayız. Bunların ruh sağlığımız üzerindeki etkilerini ihmal etmemeliyiz. İş zamanlarımızda kurumlarımızın mevcut kurallarına uyuyorsak, kişisel yaşamlarımızda da iyi bir dijital hijyen uygulamalıyız. Ekran başında geçirdiğiniz süreye dikkat etmek, sosyal medyada aşırı maruziyetten ve fazla zaman geçirmekten kaçınmak ve hesaplarınız için bir şifre yöneticisi ve iki faktörlü kimlik doğrulama kullanmak size sadece güvenlik sağlayacaktır.

İyi dijital hijyen uygulamalarının hayata geçirilmesi yalnızca çalışanların üretkenliği ve morali için fayda sağlar. Dikkat dağınıklığı azalır ve çalışanlar sürekli olarak güvenlik sorunlarıyla uğraşmadıklarında daha üretken olabilirler. Güvenli bir dijital ortam olumlu bir işyeri atmosferini teşvik eder ve morali yükseltir.

Ayrıca, dijital hijyen uygulamalarını hayata geçirmenin ve sürdürmenin ek faydalarından da bahsedebiliriz:

- **Verimli iş akışı.** Dijital varlıkların ve dosyaların uygun şekilde düzenlenmesi, iş süreçlerini kolaylaştırarak çalışanların bilgileri hızlı bir şekilde bulmasını ve görevleri daha verimli bir şekilde tamamlamasını sağlayabilir.
- **İşbirliği.** Ortak çalışma araçları ve bulut depolama kullanımı gibi dijital hijyen uygulamaları, iletişim ve dosya paylaşımı için merkezi bir platform sağlayarak ekip çalışmasını geliştirir.
- **Büyüme ve ölçeklenebilirliğe kolay adaptasyon**. Ölçeklenebilir dijital çözümlerin en başından itibaren uygulanması, girişimlerin önemli kesintiler olmadan veya dijital altyapının büyük ölçüde elden geçirilmesine gerek kalmadan büyümesine olanak tanır.
- **Esneklik.** Temiz ve düzenli bir dijital ortamın sürdürülmesi**, değişen iş ihtiyaçlarına ve pazar trendlerine** uyum sağlama esnekliği sağlar**.**
- **Çeviklik.** Çeviklikleriyle bilinen startup'lar, iyi uygulanmış bir politikanın sağladığı verimli iş akışları ve işbirliğinden yararlanır.

Özetle, girişimler için dijital hijyen politikası güvenlik, güven oluşturma, ölçeklenebilirlik, maliyet etkinliği ve operasyonel verimlilik için temel bir unsur olarak hizmet eder. Günümüzün dijital iş ortamında girişimin

sürdürülebilir başarısı ve büyümesi için çok önemli olan sorumlu ve güvenli dijital uygulamaların tonunu belirlemeye yardımcı olur.

Ünite 3 - Dijital Hijyeni İhmal Etmenin Potansiyel Tehditleri ve Sonuçları

Mart 2023'te Avrupa Birliği Siber Güvenlik Ajansı (ENISA), üye devletler ve paydaşlar arasında gelecekteki tehditler ve karşı önlemler konusunda farkındalığı artırmak amacıyla 2030 yılı için siber güvenlik tehditleri ve zorlukları hakkında kapsamlı bir rapor yayınlamıştır (Mattioli vd., 2023). Belirlenen tehditlerin birçoğu bugün bile geçerlidir ve önümüzdeki yıllarda da önemini koruyacaktır. Ekim 2023'te aynı ajans Temmuz 2022 ve Haziran 2023 arasında rapor edilen tehditler hakkında bir rapor yayınlamıştır: ENISA Threat Landscape 2023 (Lella, 2023).

Bu raporların hedef kitlesi ve paydaşları hem kamu hem de özel sektörden olmak üzere geniş olmakla birlikte, özellikle yeni kurulan şirketler bağlamında önem taşımaktadır. Yeni kurulan işletmeler, genellikle yapıları, kaynak kısıtlamaları ve iş ortamının hızla gelişen doğası ile ilgili faktörlerin bir kombinasyonu nedeniyle siber tehditlere karşı özellikle savunmasızdır. Gelişmekte olan işletmeler faaliyetleri için teknolojiye ve çevrimiçi platformlara giderek daha fazla bel bağladıklarından, siber saldırılara karşı daha hassas hale gelmektedirler. Daha önce de belirtildiği gibi, siber tehditlerin kurbanı olmanın potansiyel sonuçları arasında veri ihlalleri, mali kayıplar, itibar zedelenmesi ve hatta iş kesintisi yer almaktadır. Start-up'lar genellikle hassas bilgileri ele alırken daha büyük kuruluşların sahip olduğu altyapı ve kaynaklardan yoksundur, bu da onları güvenlik açıklarından yararlanmak isteyen siber suçlular için cazip hedefler haline getirir.

Yeni kurulan şirketlerin siber tehditlere karşı savunmasızlığı, ekonominin geneli ve diğer çeşitli kamu yapıları üzerinde de önemli etkilere sahip olabilir. Örneğin, yeni kurulan şirketlerin güvenlik açıklarının daha geniş ekonomik ve toplumsal unsurları etkileyebileceği çeşitli yollar arasında ekonomik kayıplar, iş kayıpları ve işsizlik, inovasyonun yavaşlaması, fikri mülkiyet kaybı, müşteri güveninin erozyona uğraması, tedarik zincirinde aksamalar, düzenleyici ve yasal sonuçlar, artan devlet müdahalesi ve hatta ulusal güvenlik endişeleri sayılabilir. Bu nedenle, startup'ların kendilerini ve genel olarak toplumu korumak için mevcut ve gelecekteki potansiyel tüm tehditleri kabul etmeleri ve bunlara ilişkin farkındalığı artırmaları gerekmektedir.

Siber tehditlerin kapsamlı bir şekilde anlaşılması ve sağlam güvenlik önlemlerinin uygulanması, start-up'ların riskleri azaltması ve dijital alanda uzun vadeli başarı için dayanıklı bir temel oluşturması için zorunludur. Siber tehditlerin çeşitliliği konusunda farkındalık yaratmaya yardımcı olmak için, "ENISA Threat Landscape 2023" raporunda (Lella, 2023) yer alan tehditleri aşağıda sunacağız.

Raporda yer alan başlıca tehditler Fidye Yazılımı, Kötü Amaçlı Yazılım, Sosyal Mühendislik, Verilere Yönelik Tehditler, Hizmet Reddi, İnternet Tehditleri, Bilgi Manipülasyonu ve Tedarik Zinciri Saldırılarıdır. Bunları kısaca tanımladıktan sonra "ENISA Threat Landscape 2023" raporundaki tanımlara yer verdik.

1. **Fidye yazılımı.** Fidye yazılımı, saldırgana bir miktar para veya fidye ödenene kadar bir bilgisayar sistemine veya dosyalara erişimi engellemek için tasarlanmış kötü amaçlı bir yazılım türüdür. Dosyaları şifreleyerek kurban için erişilemez hale getirebilir.
2. **Kötü Amaçlı Yazılım.** Kötü amaçlı yazılımın kısaltması olan malware, bir bilgisayar sistemine zarar vermek, veri çalmak veya normal işlemleri bozmak amacıyla oluşturulan herhangi bir yazılım veya kodu tanımlamak için kullanılan bir terimdir. Virüsler, solucanlar ve truva atları gibi çeşitli türleri içerir.
3. **Sosyal Mühendislik.** Sosyal mühendislik, hassas bilgileri ifşa etmeleri veya güvenliği tehlikeye atabilecek eylemleri gerçekleştirmeleri için bireyleri manipüle etme yöntemidir. Teknikler arasında kimlik avı, taklit ve insan davranışını istismar etmek için psikolojik manipülasyon yer alır.
4. **Verilere yönelik tehditler.** Verilere yönelik tehditler, verilerin gizliliğini, bütünlüğünü veya kullanılabilirliğini tehlikeye atan kasıtlı veya kasıtsız eylemleri kapsar. Buna veri ihlalleri, sızıntılar veya hassas bilgilere yetkisiz erişim veya ifşa da dahildir.
5. **Hizmet Reddi (DoS).** Hizmet Reddi, bir bilgisayar sisteminin, ağın veya hizmetin normal işleyişini bozmayı veya devre dışı bırakmayı amaçlayan ve bu sistemi kullanıcılar için geçici veya süresiz olarak kullanılamaz hale getiren bir saldırıdır. Dağıtılmış Hizmet Reddi (DDoS), saldırıyı koordine eden birden fazla sistemi içerir.
6. **İnternet tehditleri.** İnternet tehditleri, İnternet veya elektronik iletişimin kasıtlı veya kasıtsız olarak kesintiye uğratılması, karartılması, kapatılması veya sansürlenmesi anlamına gelir. Bu tehditler siber saldırılar, teknik sorunlar veya hükümet tarafından yönlendirilen eylemler gibi çeşitli faktörlerden kaynaklanabilir.
7. **Bilgi Manipülasyonu.** Bilgi Manipülasyonu, değerleri, prosedürleri ve siyasi süreçleri olumsuz yönde etkilemeye yönelik kasıtlı, koordineli çabaları içerir. Bu, yanlış bilgi, yalan haber yaymayı veya kamuoyunu manipüle eden veya normal bilgi akışını bozan faaliyetler yürütmeyi içerebilir.
8. **Tedarik Zinciri Saldırıları.** Tedarik Zinciri Saldırıları, kuruluşlar ile tedarikçileri arasındaki ilişkiyi hedef alır. Bu saldırılar, hedef kuruluş üzerinde yetkisiz erişim veya etki elde etmek için tedarik zincirinin güvenliğini tehlikeye atmayı içerir. Örnekler arasında yazılım güncellemelerinin veya donanım bileşenlerinin tehlikeye atılması yer alır.

"ENISA Threat Landscape 2023" raporunda tanımlanan Başlıca Tehditler

"Fidye Yazılımı

ENISA'nın Fidye Yazılımı Saldırıları için Tehdit Ortamı raporuna göre fidye yazılımı, tehdit aktörlerinin bir hedefin varlıklarının kontrolünü ele geçirdiği ve varlığın kullanılabilirliğinin iadesi karşılığında fidye talep ettiği bir saldırı türü olarak tanımlanmaktadır. Bu eylemden bağımsız tanım, değişen fidye yazılımı tehdit ortamını, birden fazla gasp tekniğinin yaygınlığını ve faillerin yalnızca finansal kazançlar dışındaki çeşitli hedeflerini kapsamak için gereklidir. Fidye yazılımları, raporlama döneminde bir kez daha, yüksek profilli ve kamuoyuna mal olmuş birkaç olayla birlikte başlıca tehditlerden biri olmuştur.

Kötü Amaçlı Yazılım

Kötü amaçlı kod ve kötü amaçlı mantık olarak da adlandırılan kötü amaçlı yazılım, bir sistemin gizliliği, bütünlüğü veya kullanılabilirliği üzerinde olumsuz bir etkiye sahip olacak yetkisiz bir işlemi gerçekleştirmeyi amaçlayan herhangi bir yazılımı veya ürün yazılımını tanımlamak için kullanılan kapsayıcı bir terimdir.

Sosyal Mühendislik

Sosyal mühendislik, bilgi veya hizmetlere erişim elde etmek amacıyla insan hatasından veya insan davranışından yararlanmaya çalışan geniş bir faaliyet yelpazesini kapsar. Kurbanları hata yapmaları ya da hassas veya gizli bilgileri vermeleri için kandırmak amacıyla çeşitli manipülasyon biçimleri kullanır. Kullanıcılar belgeleri, dosyaları veya e-postaları açmaları, web sitelerini ziyaret etmeleri veya sistemlere ya da hizmetlere erişim izni vermeleri için kandırılabilir. Kullanılan tuzaklar ve hileler teknolojiyi kötüye kullansa da, başarılı olmak için insan unsuruna dayanırlar. Bu tehdit kanvası temel olarak şu saldırı vektörlerinden oluşur: oltalama, zıpkınla oltalama, balina avcılığı, smishing, vishing, sulama deliği saldırısı, yemleme, bahane uydurma, quid pro quo, honeytraps ve scareware. Sosyal mühendislik teknikleri genellikle ilk erişimi elde etmek için kullanılırken, bir olayın veya ihlalin sonraki aşamalarında da kullanılabilirler. Önemli örnekler arasında iş e-postalarının ele geçirilmesi (BEC), dolandırıcılık, kimliğe bürünme, sahtecilik ve son zamanlarda gasp sayılabilir.

Verilere yönelik tehditler

GDPR'de veri ihlali, iletilen, depolanan veya başka bir şekilde işlenen kişisel verilerin kazara veya

yasa dışı olarak imha edilmesine, kaybolmasına, değiştirilmesine veya yetkisiz olarak ifşa edilmesine veya bunlara erişilmesine yol açan herhangi bir güvenlik ihlali olarak tanımlanmaktadır (GDPR madde 4.12). Teknik açıdan bakıldığında, verilere yönelik tehditler temel olarak veri ihlalleri veya veri sızıntıları olarak sınıflandırılabilir. Genellikle birbirinin yerine kullanılan kavramlar olsalar da, çoğunlukla nasıl gerçekleştiklerine bağlı olarak temelde farklı kavramlar içerirler. Veri ihlali, bir siber suçlu tarafından yetkisiz erişim elde etmek ve hassas, gizli veya korunan verileri serbest bırakmak amacıyla gerçekleştirilen kasıtlı bir siber saldırıdır. Başka bir deyişle, veri ihlali, veri çalmak amacıyla bir sisteme veya kuruluşa yönelik kasıtlı ve güçlü bir saldırıdır. Veri sızıntısı, hassas, gizli veya korunan verilerin kasıtsız olarak kaybolmasına veya açığa çıkmasına neden olabilecek bir olaydır (örneğin yanlış yapılandırmalar, güvenlik açıkları veya insan hataları) (kasıtlı saldırılar bazen veri açığa çıkması olarak adlandırılır).

Kullanılabilirliğe karşı tehditler: Hizmet Reddi

Kullanılabilirlik, DDoS'un da aralarında bulunduğu çok sayıda tehdit ve saldırının hedefidir. DDoS, sistem ve veri kullanılabilirliğini hedef alır ve yeni bir tehdit olmamasına rağmen siber güvenlik tehdit ortamında önemli bir rol oynar6 7. Saldırılar, bir sistemin veya hizmetin kullanıcıları ilgili verilere, hizmetlere veya diğer kaynaklara erişemediğinde meydana gelir. Bu, hizmetin ve kaynaklarının tüketilmesi ya da ağ altyapısının bileşenlerine aşırı yükleme yapılması yoluyla gerçekleştirilebilir8.

Kullanılabilirliğe karşı tehditler: İnternet tehditleri

İnternet kullanılabilirliğine yönelik tehditler, İnternet kesintileri, elektrik kesintileri, kapatmalar veya sansürle sonuçlanan kasıtlı veya kasıtsız İnternet veya elektronik iletişim kesintilerini ifade eder. İnternet kesintileri hükümet tarafından yönlendirilen internet kesintileri, kasırgalar, büyük depremler, elektrik kesintileri, kablo kesintileri, siber saldırılar, teknik sorunlar ve askeri eylemlerden kaynaklanabilir. Bu tehditler çeşitlenmekte ve büyümekte olup, bu raporlama döneminde yeni bir rekora ulaşmış ve ulusal ekonomilerde büyük parasal kayıplara neden olmuştur.

Bilgi Manipülasyonu

Yabancı Bilgi Manipülasyonu ve Müdahalesi (FIMI) değerleri, prosedürleri ve siyasi süreçleri

tehdit eden veya olumsuz etkileme potansiyeline sahip çoğunlukla yasadışı olmayan bir davranış biçimini tanımlar. Bu tür faaliyetler manipülatif niteliktedir ve kasıtlı ve koordineli bir şekilde yürütülür. FIMI, devlet veya devlet dışı aktörler tarafından, kendi toprakları içindeki ve dışındaki vekilleri de dahil olmak üzere gerçekleştirilebilir, ancak bu raporda tehdidi kaynağından bağımsız olarak inceliyoruz.

Tedarik Zinciri Saldırıları

Bir tedarik zinciri saldırısı, kuruluşlar ve tedarikçileri arasındaki ilişkiyi hedef alır. Bu ETL raporunda, ENISA Tedarik Zinciri Saldırıları için Tehdit Manzarası'nda10 belirtildiği gibi bir saldırının en az iki saldırının birleşiminden oluşması halinde tedarik zinciri bileşenine sahip olduğu kabul edilen tanımı kullanıyoruz. Bir saldırının tedarik zinciri saldırısı olarak sınıflandırılabilmesi için hem tedarikçinin hem de müşterinin hedef olması gerekmektedir. SolarWinds bu tür saldırıları ilk ortaya çıkaranlardan biri oldu ve tedarik zinciri saldırılarının potansiyel etkisini gösterdi. Tehdit aktörlerinin, bu tür saldırıların yaygın etkisinden ve geniş kurban tabanından faydalanmak amacıyla operasyonlarını yürütmek ve kurumlar içinde yer edinmek için bu kaynaktan beslenmeye devam ettikleri gözlemlenmiştir."

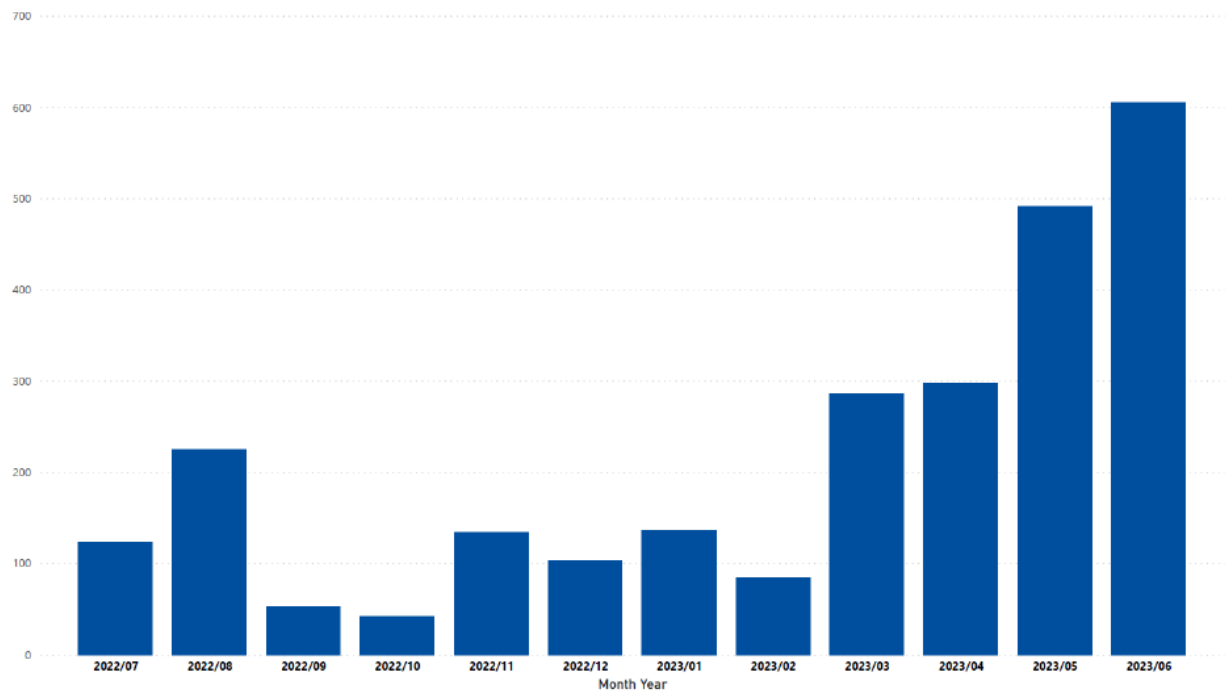
Lella, I.; Tsekmezoglou, E.; Theocharidou, M.; Magonara, E.; Malatras, A.; Naydenov, R.S.; Ciobanu, C. (2023). ENISA Tehdit Manzarası 2023. ENISA, s. 6-8

Yukarıda tanımlanan siber tehditlere (Fidye Yazılımı, Kötü Amaçlı Yazılım, Sosyal Mühendislik, Verilere yönelik tehditler, Hizmet Reddi, İnternet tehditleri, Bilgi Manipülasyonu ve Tedarik Zinciri Saldırıları) ek olarak, startup'lar çeşitli başka siber güvenlik tehditleriyle de karşı karşıya kalabilir. Farkında olunması gereken bazı ek tehditler şunlardır:

1. **Oltalama Saldırıları.** Kimlik avı, bireyleri kandırarak kullanıcı adları, parolalar veya finansal bilgiler gibi hassas bilgileri ifşa etmelerini sağlamak için aldatıcı e-postaların, mesajların veya web sitelerinin kullanılmasını içerir. Oltalama saldırıları yüksek hedefli (spear-phishing) veya daha yaygın olabilir.
2. **Ortadaki Adam (MitM) Saldırıları.** MitM saldırılarında, yetkisiz bir varlık iki taraf arasındaki iletişimi keser ve potansiyel olarak değiştirir. Bu durum veri hırsızlığına, gizli dinlemeye veya iletişim akışına kötü niyetli içerik eklenmesine yol açabilir.

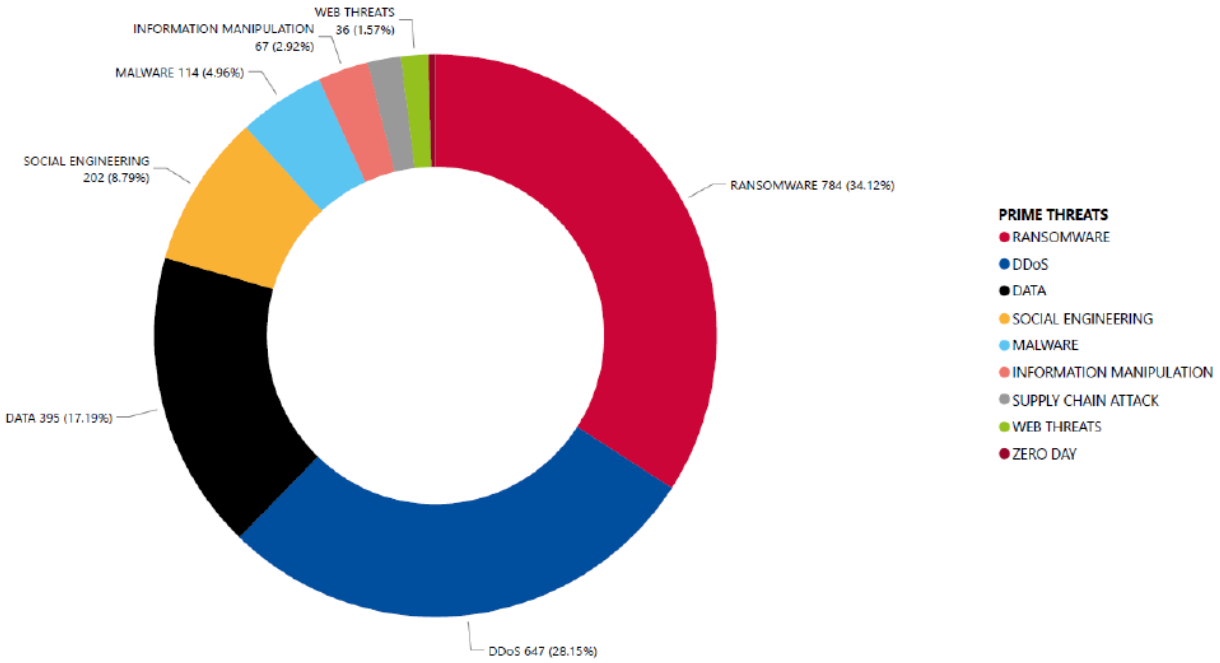
3. **Sıfır Gün Açıkları.** Sıfırıncı gün açıkları, satıcı tarafından bilinmeyen ve yaması yapılmamış yazılım açıklarıdır. Tehdit aktörleri, bir düzeltme geliştirilmeden önce bu güvenlik açıklarından faydalanabilir ve etkilenen yazılımı kullanan herhangi bir kuruluş için risk oluşturabilir.
4. **Gelişmiş Kalıcı Tehditler (APT'ler).** APT'ler, genellikle iyi finanse edilen ve organize tehdit aktörleri tarafından düzenlenen sofistike ve hedefli siber saldırılardır. Bu saldırılar genellikle hassas bilgileri çalmayı amaçlayarak bir ağa uzun süreli ve gizli bir şekilde sızmayı içerir.
5. **IoT (Nesnelerin İnterneti) Güvenlik Açıkları.** Girişimler IoT cihazlarını operasyonlarına giderek daha fazla entegre ettikçe, bu cihazlar siber saldırılar için potansiyel hedefler haline gelebilir. Güvensiz IoT cihazları, ağlara yetkisiz erişim sağlamak veya saldırılar başlatmak için istismar edilebilir.
6. **Cryptojacking.** Cryptojacking, kripto para madenciliği yapmak için bir bilgisayarın veya ağın kaynaklarının yetkisiz kullanımını içerir. Siber suçlular, sistemlere sessizce kripto para madenciliği yapan ve sistem performansını etkileyen kötü amaçlı yazılımlar bulaştırabilir.
7. **Siteler Arası Komut Dosyası Yazma (XSS).** XSS saldırıları, diğer kullanıcılar tarafından görüntülenen web sayfalarına kötü amaçlı komut dosyaları enjekte etmeyi içerir. Bu, kullanıcı verilerinin çalınmasına, oturumun ele geçirilmesine veya kötü amaçlı yazılımların diğer kullanıcılara yayılmasına yol açabilir.
8. **SQL Enjeksiyonu.** SQL enjeksiyon saldırıları, kötü niyetli SQL kodunun girdi alanlarına enjekte edilerek saldırganların bir veritabanını manipüle etmesine izin vermesiyle ortaya çıkar. Bu durum yetkisiz erişime, veri manipülasyonuna veya veri çıkarımına yol açabilir.
9. **Dosyasız Kötü Amaçlı Yazılım.** Dosyasız kötü amaçlı yazılımlar çalıştırılabilir dosyalara dayanmak yerine bellekte çalışır. Bu, analiz edilecek fiziksel bir dosya olmayabileceğinden geleneksel antivirüs çözümlerinin tespit etmesini daha zor hale getirir.
10. **Kimlik Bilgisi Doldurma.** Kimlik bilgisi doldurma saldırılarında siber suçlular, kullanıcıların kimlik bilgilerini yeniden kullandığı başka bir hizmete yetkisiz erişim sağlamak için bir hizmetten çalınan kullanıcı adı ve parola kombinasyonlarını kullanır.
11. **DNS Sahtekarlığı ve Önbellek Zehirlenmesi.** DNS sahtekarlığı, alan adı sistemi (DNS) sorgularının kötü amaçlı sitelere yönlendirilmesini içerir. Önbellek zehirlenmesi, DNS önbellek verilerini manipüle ederek kullanıcıları istenmeyen ve potansiyel olarak zararlı hedeflere yönlendirir.

Belirtildiği üzere, "ENISA Threat Landscape 2023" raporu (Lella, 2023) dünya genelinde ve AB'de başlıca tehditlerin şunlar olduğunu göstermektedir: Fidye yazılımları, Kötü Amaçlı Yazılımlar, Sosyal Mühendislik, Verilere yönelik tehditler, Hizmet Reddi, İnternet tehditleri, Bilgi Manipülasyonu ve Tedarik Zinciri Saldırıları.



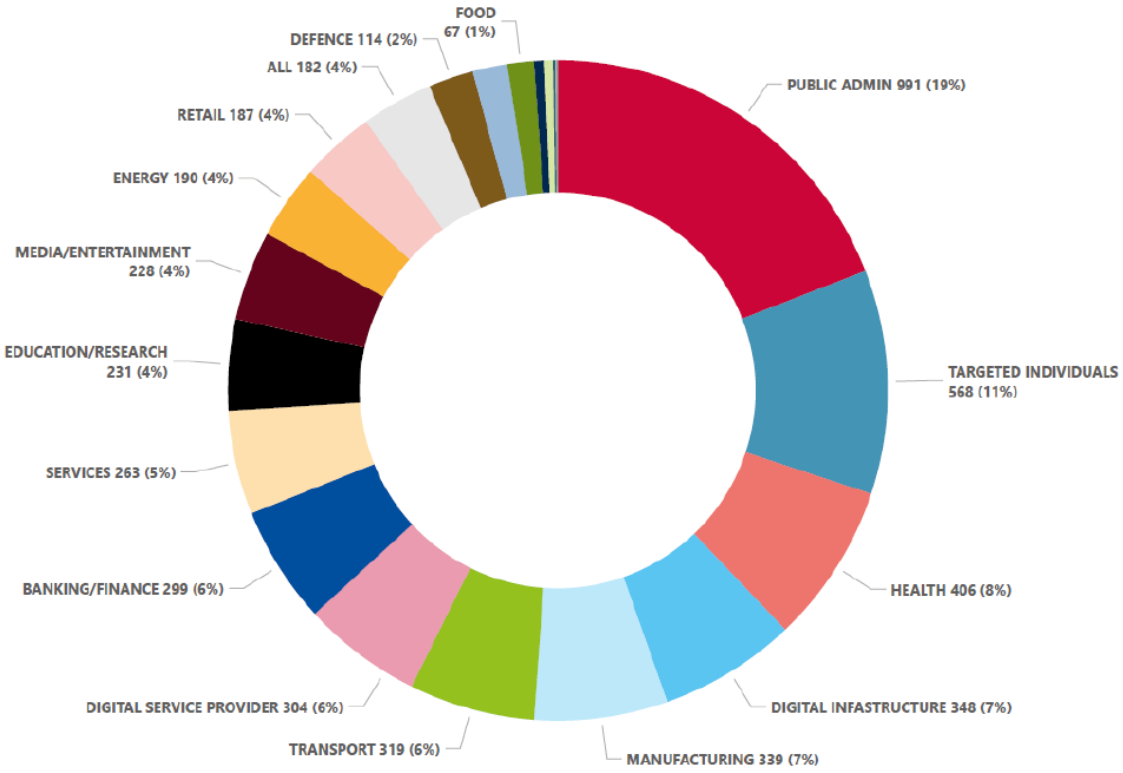
Şekil 1. AB olaylarının zaman çizelgesi AB olaylarının zaman çizelgesi (ay başına gözlemlenen olay sayısı) (Lella, 2023)

Rapor, 2023'ün ilk bölümünde siber saldırılardaki artışı göstermektedir (Şekil 1). Bu artış hem küresel hem de AB düzeyinde görülmektedir. Artış sadece sayılardaki artışı değil, aynı zamanda bu tür olayların gerçekleştiğine dair farkındalığı da yansıtıyor olabilir. Yine de bu eğilim endişe vericidir.



Şekil 2. Tehdit gruplarına göre Tehdit grubuna göre tehdit sayısının AB dağılımı (Lella, 2023)

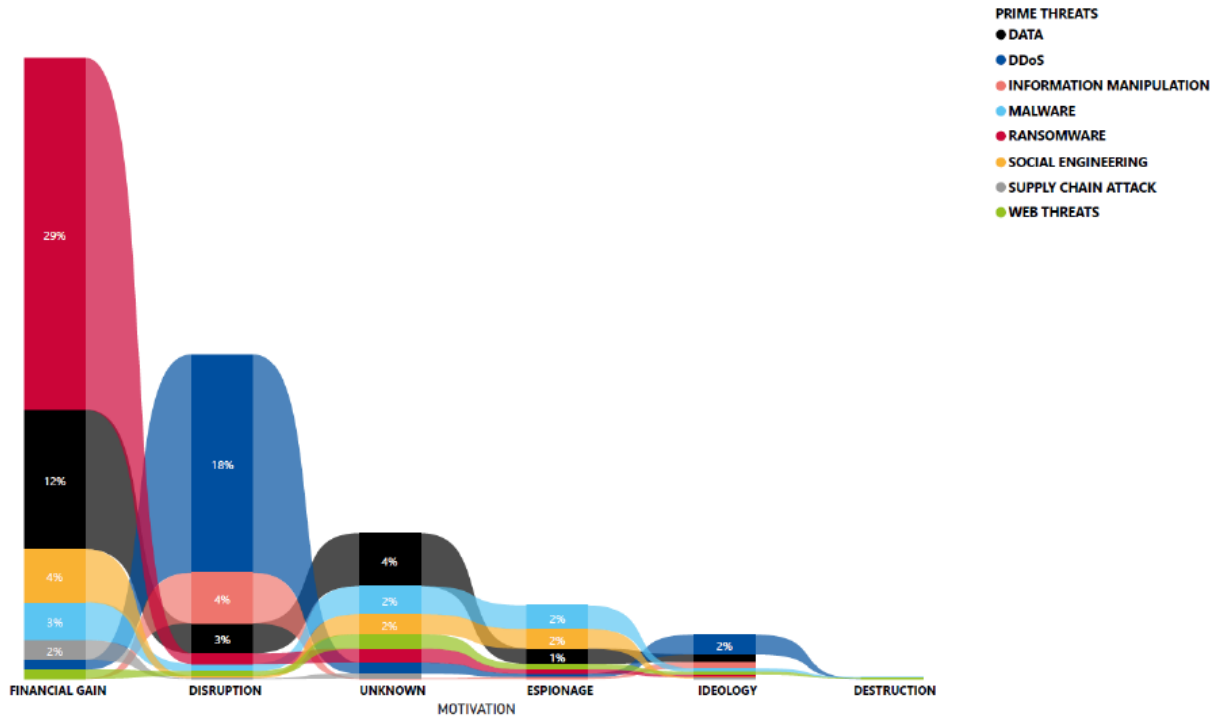
Şekil 2'de en sık karşılaşılan tehditlerin şunlar olduğunu görebiliriz: Fidye yazılımları, Hizmet Reddi, Verilere yönelik tehditler, Sosyal Mühendislik ve Kötü Amaçlı Yazılımlar. Bunları Bilgi Manipülasyonu, Tedarik Zinciri Saldırıları, İnternet tehditleri ve Sıfırıncı Gün takip etmektedir.



Şekil 3. Olay sayısı başına hedeflenen sektörler (Temmuz 2022 - Haziran 2023) (Lella, 2023)

Sektörel bir analiz, tehditlerin belirli endüstrilerin veya sektörlerin sınırlarını aştığını ve etkilerini geniş bir alan yelpazesinde gösterdiğini ortaya koymaktadır (Lella, 2023). Bu durum, günümüz dijital dünyasının birbiriyle olan yüksek bağlanabilirliğinden kaynaklanıyor olabilir.

Genel küresel manzarada, çok sayıda olay kamu yönetimi (%19) ve sağlık (%8) sektörlerindeki kuruluşları hedef almıştır. Tehdit edilen ana aktörlerden birinin de bireyler olduğunu görüyoruz (%11). Bu durum startup'lar ve özel sektörle ilgisiz gibi görünse de, bu bireyler bazı startup şirketlerinde çalışan olabilir ve istemeden de olsa şirketleri riske atabilirler.



Şekil 4. Tehdit kategorilerine göre Tehdit kategorisine göre tehdit aktörlerinin motivasyonu (Lella, 2023)

Rapor aynı zamanda belirlenen dönemdeki siber saldırıların arkasındaki motivasyonları da sunmaktadır (Lella, 2023). Şekil 4'ten de görülebileceği üzere, saldırıların çoğunda finansal kazanç elde edilmiş, bunu kesinti, bilinmeyen, casusluk ve ideoloji izlemiştir. Fidye yazılımları, finansal kazanç için gerçekleştirilen saldırıların neredeyse %30'unu oluştururken, bunu verilere yönelik tehditler, sosyal mühendislik ve kötü amaçlı yazılımlar takip etmektedir.

Siber tehditlerin arkasındaki nedenlerin ve tehdit türlerinin farkında olmak, girişimlerin dijital hijyen uygulamaları geliştirmek ve uygulamak için kullandıkları stratejiyi bilgilendirebilir ve yönlendirebilir. Örneğin, girişimler ve özel sektör çoğunlukla finansal kazançlar için hedef alınmaktadır. Fidye yazılımları, verilere yönelik tehditler, sosyal mühendislik ve kötü amaçlı yazılımların ağırlıklı olarak bu tür amaçlar için kullanıldığını bilen startup'lar, dijital hijyen stratejilerini verilere erişimi korumaya ve müşterilerin ve çalışanların kendilerini sosyal mühendislik tehditlerinden korumaları için eğitilmelerine odaklayabilir.

Bir girişimin siber tehditlere nasıl yaklaşması gerektiğini ve kendilerini korumak için neler yapmaları gerektiğini anlamaya yardımcı olmak için bir iyi uygulama örneği hazırladık. Bu, bir şirketin olası tehditlerle nasıl başa çıkması gerektiğini ve siber olayların meydana gelmesini önlemek için nasıl hazırlanması gerektiğini gösterecektir.

Ünite 4 - Yeni kurulan şirketlerden iyi uygulamalar

Tehditlerin nasıl tespit edileceğini ve durumun önceden nasıl ele alınacağını daha iyi anlamak için aşağıdaki örneği ele alalım. Örneği, bir siber saldırı durumunda hem şirketi hem de müşterileri etkileyebilecek yaygın ve yaygın bir durum olan çevrimiçi ödemeden kaynaklanabilecek güvenlik açığına odakladık.

Online Ödeme Güvenliğinde Dijital Hijyen

Bağlam

İnovasyonun finansal işlemlerle kesiştiği mobil uygulama geliştirmenin hızla gelişen ortamında, çevrimiçi ödemeleri işleyen bir uygulamanın güvenliğini sağlamak çok önemli hale geliyor. Örnek olarak, mobil uygulama aboneliği sunan bir şirketin ödeme işlemleriyle ilgili bir güvenlik açığı ortaya çıkabilir. Çevrimiçi ödeme işleme sistemlerindeki potansiyel güvenlik açığı, hem şirketi hem de müşterilerini finansal dolandırıcılık risklerine maruz bırakabilir.

Girişimin durumu analiz etmesi, riskleri belirlemesi ve herhangi bir güvenlik açığı ve mali dolandırıcılık durumunu önlemek için çözümler uygulaması gerekir.

1. Adım. Durum Analizi

Dijital hijyen sürecinin ilk adımı olarak durum analizine sahibiz. Bu aşamada, güvenlik açıklarının belirlenmesi ve bir güvenlik ihlali durumunda bu açıkların risk ve etkilerinin değerlendirilmesi önemlidir.

Ödeme Güvenliği Zafiyetinin Belirlenmesi:

Şirket, güvensiz ödeme ağ geçitleri, işlem şifrelemesindeki açıklar ve yetkisiz erişimin olası noktaları da dahil olmak üzere potansiyel zayıf noktaları belirlemek için uygulamanın ödeme işleme işlevselliğinin kapsamlı bir analizini gerçekleştirdi.

Potansiyel zayıf noktaları belirlemek için bir ödeme uygulamasının kapsamlı bir analizinin yapılması, uygulama içindeki çeşitli bileşenlerin sistematik ve kapsamlı bir şekilde incelenmesini gerektirir. Böyle bir analizin yürütülmesi için genel bir kılavuz şunları içerebilir:

1. **Risk Değerlendirmesi:** Kullanıcı kimlik doğrulaması, veri depolama, ödeme işleme ve harici sunucularla iletişim dahil olmak üzere ödeme uygulamasının kritik bileşenlerini belirleyin ve anlayın.
2. **Mevzuata Uygunluk Kontrolü:** Ödeme uygulamasının, Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (PCI DSS) gibi sektördeki ilgili düzenleyici standartlara ve uyumluluk gereksinimlerine uygun olduğundan emin olun.
3. **Veri Akışı Haritalaması:** Hassas verilerin (ör. kredi kartı bilgileri) uygulama içindeki akışını, girişten depolamaya ve iletime kadar haritalayın. Bu veri akışındaki potansiyel güvenlik açığı noktalarını belirleyin.
4. **Ağ Güvenliği:** Güvenli protokollerin (HTTPS), şifrelemenin ve güvenli yuva katmanı (SSL) sertifikalarının kullanımı da dahil olmak üzere ağ iletişimlerinin güvenliğini değerlendirin.
5. **Kimlik Doğrulama Mekanizmaları:** Kullanıcı kimlik doğrulama mekanizmalarının gücünü değerlendirin. Ekstra bir güvenlik katmanı eklemek için çok faktörlü kimlik doğrulama uygulayın.
6. **Ödeme Ağ Geçidi Güvenliği:** Güvenli ve saygın hizmetlerin kullanıldığından emin olmak için ödeme ağ geçitleri ile entegrasyonu inceleyin. Ödeme ağ geçidi yazılımını düzenli olarak güncelleyin ve yama uygulayın.
7. **Veri Şifreleme:** Hassas kullanıcı verilerini tüm işlem süreci boyunca korumak için uçtan uca şifreleme uygulayın.
8. **Güvenlik Açığı Taraması ve Sızma Testi:** Potansiyel zayıflıkları belirlemek ve gerçek dünya saldırı senaryolarını simüle etmek için düzenli güvenlik açığı taramaları ve sızma testleri yapın. Bu, otomatik araçlar kullanmayı veya sızma testi konusunda uzman üçüncü taraf güvenlik firmalarını işe almayı içerebilir.
9. **Kod İncelemesi:** Uygulamanın kaynak kodundaki güvenlik açıklarını veya zayıflıkları belirlemek için kapsamlı bir kod incelemesi gerçekleştirin. Kodlama uygulamalarının en iyi güvenlik uygulamalarına uygun olduğundan emin olun.
10. **Olay Müdahale Planı:** Olası güvenlik ihlallerini derhal ele almak ve azaltmak için bir olay müdahale planı geliştirin ve uygulayın. Bu, bir güvenlik olayı durumunda kullanıcıları bilgilendirmek için prosedürlerin uygulanmasını da içerir.
11. **Üçüncü Taraf Güvenlik Denetimleri:** Uygulama güvenliği denetimlerinde uzmanlaşmış üçüncü taraf güvenlik firmalarıyla çalışmayı düşünün. Bu firmalar, güvenlik açıklarını tespit etmek için bağımsız bir bakış açısı ve uzmanlık getirebilir.

Analizinizi gerçekleştirmek için bu noktaları bir kontrol listesi olarak kullanabilirsiniz.

Güvenlik devam eden bir süreçtir ve düzenli gözden geçirmeler ve güncellemeler ortaya çıkan tehditlerin önüne geçmek için çok önemlidir. Yukarıda belirtilen kontrol listesindeki noktalar, olası tehditlere ve siber güvenlik ortamına göre zaman içinde değişebilir. Üçüncü taraf güvenlik firmaları veya danışmanlarla

çalışmak, özellikle kapsamlı güvenlik denetimleri ve sızma testleri söz konusu olduğunda ek uzmanlık ve içgörü sağlayabilir. Hem işletmeyi hem de kullanıcılarını potansiyel risklerden ve ihlallerden korumak için ödeme uygulamalarının güvenliğine öncelik vermek çok önemlidir.

Rutin bir güvenlik denetimi sırasında, startup güvenlik ekibinin mobil uygulamalarında ödeme verilerini iletmek için kullanılan şifreleme protokolünde potansiyel bir zayıflık tespit ettiğini varsayalım. Ardından, ekibin bu güvenlik açığını ve bunun şirket ve kullanıcılar üzerindeki etkilerini değerlendirmesi gerekiyor.

Risklerin ve Etkilerin Değerlendirilmesi:

Ödeme güvenliği açıklarını belirledikten sonra, hem şirket hem de kullanıcılar için riskleri ve sonuçları dikkate almak önemlidir. Sürecin bu kısmı, şirket ve kullanıcılar için risklerin değerlendirilmesini ve belirlenen güvenlik açıklarının potansiyel etkiye göre önceliklendirilmesini içerir.

1. **Etki değerlendirmesi:** Bir güvenlik ihlalinin hem şirket hem de kullanıcılar üzerindeki potansiyel etkisini, mali kayıpları, itibar zedelenmesini ve olası yasal sonuçları göz önünde bulundurarak değerlendirin.
2. **Önceliklendirme:** Güvenlik açıklarını potansiyel etkinin ciddiyetine ve istismar olasılığına göre önceliklendirin.

Şifreleme protokolündeki zayıflıkla ilişkili risklerin değerlendirilmesi sırasında güvenlik ekibi, kullanılan şifreleme algoritmasının türü, potansiyel istismarın kapsamı ve kullanıcı veri güvenliği üzerindeki etkisi gibi faktörleri göz önünde bulundurarak güvenlik açığının kapsamını değerlendirir.

Risk analizi, hassas ödeme bilgilerine yetkisiz erişim riski ve şirketin itibarı üzerindeki potansiyel etki dahil olmak üzere şifreleme açığının potansiyel sonuçlarını anlamayı amaçlamaktadır.

Adım 2. Bir Çözüm Bulmak

Olası ödeme güvenliği açıkları için çözümler şunları içerir:

1. **Güvenli Ödeme Ağ Geçidi Entegrasyonu:** Ödeme işleme sistemini güvenli bir ödeme ağ geçidi ile entegre olacak şekilde yükselterek tüm işlemlerin şifrelenmesini ve iletim sırasında müdahaleye karşı korunmasını sağlayın.
2. **Uçtan Uca Şifreleme:** Tüm ödeme işlemleri için uçtan uca şifreleme uygulayarak hassas kullanıcı verilerini işlem sürecinin her aşamasında yetkisiz erişime karşı koruyun.
3. **Kullanıcı Kimlik Doğrulama Geliştirmeleri:** Yalnızca yetkili kullanıcıların uygulamaya erişebilmesini ve uygulama içinde işlem yapabilmesini sağlamak için çok faktörlü kimlik doğrulamayı içeren kullanıcı kimlik doğrulama önlemlerini güçlendirin.

4. **Düzenli Güvenlik Denetimleri ve Uyumluluk Kontrolleri:** Özellikle ödeme işleme işlevine odaklanan rutin güvenlik denetimleri gerçekleştirin, endüstri standartları ve yönetmeliklerle uyumluluk kontrolleri yapın.

Örnek olarak kullandığımız şifreleme protokolündeki zayıflığın daha spesifik bakımında, yanıt ve hafifletme şunları içerecektir:

1. **Derhal Kontrol Altına Alma:** Şirket, daha fazla potansiyel istismarı önlemek için etkilenen şifreleme protokolünü geçici olarak devre dışı bırakarak güvenlik açığını kontrol altına almak için derhal harekete geçer.
2. **Paydaşlarla İletişim:** Şirket, kullanıcılarıyla şeffaf bir iletişim başlatarak onları tespit edilen şifreleme açığı, etkilenen özelliğin geçici olarak askıya alınması ve sorunu ele almak için devam eden çabalar hakkında bilgilendirir.
3. **Güvenlik Uzmanlarının Katılımı:** Şirket, şifreleme güvenlik açığının derinlemesine bir analizini yapmak ve daha sağlam ve güvenli bir şifreleme çözümü için öneriler sunmak üzere harici siber güvenlik uzmanlarının hizmetlerinden yararlanır.
4. **Bir Yama Geliştirilmesi:** Geliştirme ekibi, güvenlik uzmanlarından gelen önerilere dayanarak şifreleme açığını gideren bir yama oluşturur. Bu, daha güvenli bir şifreleme algoritmasının uygulanmasını ve mevcut sistemlerle uyumluluğun sağlanmasını içerir.
5. **Dahili Testler:** Yamayı dağıtmadan önce şirket, güncellenen şifreleme önlemlerinin yeni güvenlik açıkları yaratmadığından veya ödeme uygulamasının işlevselliğini bozmadığından emin olmak için kapsamlı dahili testler gerçekleştirir.
6. **Yamanın Dağıtımı:** Yamanın etkili ve güvenli olduğuna karar verildiğinde, şirket güncellemeyi tüm kullanıcıların cihazlarına dağıtarak gelişmiş şifreleme önlemleri ile ödeme işlevini eski haline getirir.
7. **Uygulama Sonrası İzleme:** Şirket, şifreleme yamasının güvenlik açığını başarılı bir şekilde azalttığından ve öngörülemeyen herhangi bir soruna yol açmadığından emin olmak için uygulama sonrası uygulamanın performansını yakından izler.
8. **Kullanıcı Eğitimi:** Kullanıcı güvenini yeniden tesis etmek için şirket, uygulama içinde bir eğitim kampanyası başlatarak kullanıcıları şifreleme açığı ve bu açığı gidermek için atılan adımlar hakkında bilgilendirebilir ve güvenli kullanım uygulamalarını sürdürmeye yönelik ipuçları sağlayabilir.

Bu yanıttaki adımlar tanımlanan soruna özgüdür. Güvenlik denetiminde farklı bir sorun tespit edilirse, bu soruna yönelik özel yanıtlar devreye sokulacaktır.

3. Adım. Sonuçlar ve Etki

Şirketin çevrimiçi ödemeler için uygulama güvenliğinde dijital hijyene yönelik hedefli yaklaşımı olumlu sonuçlar verdi:

- Bir yıl boyunca sıfır yetkisiz işlem veya güvenlik ihlali vakası.
- Kullanıcıların uygulamaya olan güveninin artması, işlem sayısında ve olumlu kullanıcı yorumlarında artışa yol açtı.
- Sektör düzenlemelerine uyum, şirketin çevrimiçi ödemeler için güvenli ve güvenilir bir platform olarak konumlandırılması.

Önemli Çıkarımlar

Ödeme işleme uygulamaları sunan start-up'lar bu örnekten değerli bilgiler çıkarabilir:

- İşlem verilerini korumak için güvenli ödeme ağ geçitlerinin entegrasyonuna öncelik verin.
- Ödeme süreci boyunca kullanıcı verilerini korumak için uçtan uca şifreleme uygulayın.
- Daha fazla güvenlik için çok faktörlü kimlik doğrulamayı dahil ederek kullanıcı kimlik doğrulama önlemlerini geliştirin.
- Olası güvenlik açıklarının önüne geçmek ve endüstri standartlarıyla uyumluluğu sağlamak için düzenli güvenlik denetimleri ve uyumluluk kontrolleri gerçekleştirin.

Ödeme işleme uygulaması geliştiricileri, bu dijital hijyen uygulamalarını benimseyerek güvenli ve güvenilir bir platform oluşturulmasına katkıda bulunabilir ve çevrimiçi finansal işlemlerle ilgilenen kullanıcılar arasında güveni artırabilir.

Referanslar:

Mattioli, R.; Malatras, A.; Hunter, E.N.; Biasibetti Penso, M.G.; Bertram, D.; Neubert, I. (2023). Ortaya Çıkan Siber Güvenlik Tehditlerinin ve 2030 için Zorlukların Belirlenmesi. ENISA

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

Dijital hijyen: bitmemiş en önemli iş: https://www.telefonica.com/en/communication-room/blog/digital-hygiene-the-most-important-unfinished-business/

Siber Hijyen Nedir? Tanım, Faydalar ve En İyi Uygulamalar: https://securityscorecard.com/blog/what-is-cyber-hygiene-definition-benefits-best-practices/

Siber hijyen nedir ve neden önemlidir?

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