SİBER GÜVENLİK BİLGİLENDİRME

İçişleri Bakanlığı'nın Bilgi Güvenliği Politikaları Yönergesi ile Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve T.C. Siber Güvenlik Başkanlığı tarafından hazırlanan Kamu Bilgi ve İletişim Güvenliği Rehberi kapsamında yasal bir zorunluluk olarak kurumun tamamını kapsayacak şekilde aşağıdaki başlıklarda uygulanması gereken güvenlik tedbirleri bulunmaktadır.

- Ağ ve sistemler,
- Uygulamalar,
- Taşınabilir Cihaz ve Ortamlar,
- IoT Cihazları,
- Personel,
- Fiziksel Mekânlar

Kurumsal siber güvenliği sağlamak için sistemli ve düzgün kurgulanmış bir güvenlik yapısı kurmak gerekiyor. Bunun için Kurumsal Şifre Politikaları ve Teknik Koruma Önlemleri konularına dikkat etmek gerekiyor.

- **Kurumsal Şifre Politikaları**
    - Karmaşıklık : Şifrelerin en az 8-12 karakterden oluşması; büyük/küçük harf, rakam ve özel karakter içermesi.
    - Düzenli Değişim : Personel şifrelerinin belirli periyotlarla (örneğin 90 günde bir) değiştirilmesi.
    - Tahmin Edilebilir Şifre Yasağı : "123456", "admin" veya kurum/personel adı gibi kolay tahmin edilebilir olmaması.

- **Teknik Koruma Önlemleri**
    - Hatalı Giriş Sınırı (Lockout) : Belirli sayıda (genellikle 3 veya 5) başarısız giriş denemesinden sonra kullanıcı hesabının veya ilgili IP adresinin geçici olarak kilitlenmesi.
    - CAPTCHA Kullanımı : Üst üste hatalı deneme yapılan giriş sayfalarında bot koruma mekanizmalarının (CAPTCHA) aktif edilmesi.
    - Çok Faktörlü Kimlik Doğrulama (MFA/2FA) : Sadece şifrenin bilinmesini yetersiz kılarak SMS, e-posta veya doğrulama uygulaması kodu zorunluluğu getirilmesi.
    - IP Sınırlaması ve Engelleme : Belirli bir zaman diliminde aşırı istek gönderen (Brute Force) IP adreslerinin güvenlik duvarı (Firewall) tarafından otomatik olarak engellenmesi.

Beyaz Web yazılım ürünlerinde kullanılan tüm kütüphaneler düzenli olarak güvenlik açığı (vulnurability) kontrollerinden geçmektedir. (*https://owasp.org/www-project-dependency-check/*)

KYS uygulamasına girişte üç hatalı giriş sonrası kullanıcı hesabı kilitlenerek sistem yöneticisine yönlendirilmektedir. Kilitlenen kullanıcı hesabı sistem yöneticisi onayı ile açılabilmektedir. KYS uygulaması iç ağda yer alıyor olsa da kurumun Siber Güvenlik Yapısına dahil edilmelidir. Kullanıcıların şifrelerini birbirleri ile paylaşmaları yaygın şekilde gözlemlenmektedir. Bu nedenle KYS uygulamasında aynı kullanıcı ve şifre ile giriş yapıldığında önceki oturumlar kapatılmakta ve diğer oturum ekranlarına uyarı mesajı gönderilmektedir. Kullanıcı ekranının aniden kapandığını bildirmesi durumunda derhal Aktif Kullanıcılar sayfasından bu kullanıcının giriş yaptığı ip adresi not edilerek başka biri aynı kullanıcı ve şifre ile giriş mi yaptı kontrol edilmelidir.

E-Belediye uygulamasında Çok Faktörlü Kimlik Doğrulama (Şifre ve Sms Şifresi) kullanılmaktadır. E-Belediye uygulaması DMZ bölgesinde yayımlandığı için birçok kötü niyetli saldırılara (yaklaşık 11 adet) açık durumdadır. Bu nedenle E-Belediye uygulaması mutlaka kurumun Siber Güvenlik Yapısına dahil edilmelidir.

Siber Güvenlik Yapısına İlişkin Tavsiyeler

Siber Güvenlik Uzmanı ile beraber kurumun tamamını (tüm yazılım, donanım ve personeller) kapsayacak şekilde aşağıdaki yönergeler uygulanmalıdır. Önemsenmeyen bir açık, kurumun tüm sistemlerini savunmasız bırakabilir.

- İçişleri Bakanlığı'nın Bilgi Güvenliği Politikaları Yönergesi.
  https://www.icisleri.gov.tr/bilgiteknolojileri/yonergeler

- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve T.C. Siber Güvenlik Başkanlığı tarafından hazırlanan Kamu Bilgi ve İletişim Güvenliği Rehberi.
  https://siberguvenlik.gov.tr/faydali-dokumanlar

- Firewall'da gerekli güvenlik (DMZ, ip erişim) ayarları ile IDS (Saldırı Tespit Sistemi), IPS (Saldırı Önleme Sistemi) ve DOS Koruma Sistemleri mutlaka açık olmalıdır. Firewall aşağıdaki özelliklere haiz olmalıdır.
  - ✓ IDS/IPS (Saldırı Tespit/Önleme Sistemi)
  - ✓ Web ve uygulama filtreleme
  - ✓ VPN
  - ✓ 5651 sayılı yasaya uygun şekilde loglama
  - ✓ Siber Güvenlik Kanunu'na tam uyum

  https://berqnet.com/sertifika/firewall/firewall-ips

- Ücretsiz bir şekilde kullanılabilecek, firewall'dan daha gelişmiş IDS/IPS sistemleri mevcuttur. Bu seçenek te mutlaka değerlendirilmeli. Günümüzde en çok tercih edilen yöntem budur.
  https://developers.cloudflare.com/use-cases/solutions/stop-account-takeover-attacks/

Terimler Sözlüğü

- **Tehditler**

  - **Malware** : Kötü Amaçlı Yazılım
    Virüsler, truva atları, solucanlar ve fidye yazılımları gibi zararlı programlardır.

  - **Phishing** : Kimlik avı
    Kötü niyetli kişilerin, meşru bir kaynaktan geliyormuş gibi görünen sahte e-postalar veya mesajlar yoluyla kişisel bilgileri veya finansal verileri ele geçirme girişimidir.

  - **Zero Day Exploit** :
    Adını bir yama yayınlandıktan sonra, kullanıcıların güvenlik güncellemelerini indirirken az sayıda bilgisayara ulaşmalarından alır. Yazılımdaki açıklar henüz daha düzeltilmemiştir ve bu da saldırganlara fırsat sağlar. Bu tür güvenlik açıklarından yararlanma teknikleri günümüzde Darkweb üzerinden yayınlanmakta veya satılmaktadır.

- **Social Engineering** : Sosyal Mühendislik
  insanların güvenlik protokollerini atlatmalarını sağlamak için manipülasyon yoluyla bilgi elde etme veya sistemlere erişim sağlama yöntemidir. Bu yöntemler arasında telefonla arama, sahte kimliklerle insanları kandırma ve psikolojik manipülasyon bulunur.

- **DDoS** : Dağıtılmış Hizmet Reddi Saldırısı
  Bir ağı, hizmeti veya web sitesini aşırı yükleyerek hizmet veremez hale getirmeyi amaçlar. Saldırganlar, çok sayıda bilgisayardan veya cihazdan aynı anda hedefe büyük miktarda trafik gönderir.

- **Brute Force Attack** : Kaba Kuvvet Saldırısı
  Bir saldırganın şifreleri, kullanıcı adlarını veya şifreleme anahtarlarını bulmak için olası tüm kombinasyonları otomatik olarak veya el yordamıyla deneme yanılma yoluyla test etmesidir.

- **Man in The Middle** :
  Bu siber saldırı çeşidinde ise saldırganlar kurbanlar ile erişmek istedikleri web servisi arasında kendilerini gizleyerek, kurbanları kendi ağları üzerinden erişmek istedikleri servise yönlendirirler. Örneğin bir Wi-Fi ağını taklit ederler ve kurbanlar erişmek istedikleri Wi-Fi ağı yerine saldırganların Wi-Fi ağına girmiş olurlar. Bundan sonraki yaptıkları her işlemi saldırganlar görebilir ve kullanıcıların verilerini toplayabilirler.

- **SQL Injection** :
  Günümüzde birçok veri tabanı SQL ile yazılmış komutlara uymak için tasarlanmıştır ve kullanıcılardan bilgi alan birçok web sitesi bu verileri SQL veri tabanlarına gönderir. Saldırganlar SQL güvenlik açıklarından faydalanarak kurbanların veri tabanlarını kontrol altına alırlar. Örneğin bir SQL enjeksiyon saldırısında bir bilgisayar korsanı, bazı SQL komutlarını ad ve adres bilgisi isteyen bir web formuna yazar; web sitesi ve veri tabanı doğru programlanmadıysa, veri tabanı bu komutları çalıştırmayı deneyebilir.

- **Cryptojacking** :
  Başkasının bilgisayarının sizin için cryptocurrency üretme işini yapmasını içeren özel bir saldırıdır. Saldırganlar gerekli hesaplamaları yapmak için kurbanın bilgisayarına kötü amaçlı yazılım yüklerler veya bazen kötü amaçla kullandıkları kodları kurbanın tarayıcısında çalışan JavaScript'te çalıştırırlar.

- **Eavesdropping Attack** :
  Bu saldırı tipinde saldırganlar bir ağa sızarlar ve gizlice dinleme yaparak kullanıcıların o ağ üzerinden göndereceği kredi kartı bilgileri, şifreler ve konuşmalar gibi kişisel verileri dinlerler. Pasif olan yönteminde genellikle sadece dinleme yaparak bilgiler toplanır fakat aktif yönteminde ise saldırganlar kullanıcılara ağdaki dost bir birim gibi gözükerek sorular sorarak bilgi toplarlar.

- **Birthday Attack** :
  Bir mesajın, yazılımın veya dijital imzanın bütünlüğünü doğrulamak için kullanılan karma algoritmalara karşı yapılır. Bir karma işlevi tarafından işlenen bir mesaj, giriş mesajının uzunluğundan bağımsız olarak sabit uzunlukta bir mesaj özeti (MD) üretir. Bu MD, mesajı benzersiz bir şekilde karakterize eder. Doğum günü saldırısı, bir karma işlevi tarafından işlendiğinde aynı MD'yi üreten iki rastgele mesaj bulma olasılığını ifade eder. Bir

saldırgan, kullanıcısı olduğu gibi mesajı için aynı MD'yi hesaplarsa, kullanıcının mesajını güvenle onunla değiştirebilir ve alıcı MD'leri karşılaştırsa bile değiştirmeyi tespit edemez.

- **Savunma**

  - **Firewall** : Güvenlik duvarı
    Ağ trafiğini filtrelemek ve iç ağları dış tehditlerden korumak için kullanılır. Aşağıdaki özelliklere sahip olmalıdır.
    - ✓ IDS/IPS (Saldırı Tespit/Önleme Sistemi)
    - ✓ Web ve uygulama filtreleme
    - ✓ VPN
    - ✓ 5651 sayılı yasaya uygun şekilde loglama
    - ✓ Siber Güvenlik Kanunu'na tam uyum

  - **IDS/IPS** : Saldırı tespit ve önleme sistemi
    Ağ trafiğini izleyerek potansiyel saldırıları tespit eden ve engelleyen güvenlik çözümleridir. IDS, tehditleri algılar ve raporlar; IPS ise tespit edilen tehditleri otomatik olarak engeller. IPS sistemi, bir ağ saldırısını tespit ettiğinde, saldırıyı durdurmak için trafiği otomatik olarak bloke edebilir.

  - **Antivirüs yazılımı** :
    Virüsler, truva atları, solucanlar ve fidye yazılımları tespit etmek, engellemek ve temizlemek için kullanılan programlardır.

  - **Encryption** : Şifreleme
    Verilerin yetkisiz erişimden korunması için okunamaz hale getirilmesi işlemidir.

  - **Strong password** : Güçlü şifre
    Büyük harf, küçük harf, rakam ve semboller içeren, tahmin edilmesi zor şifrelerdir.

  - **MFA** : Çok faktörlü kimlik doğrulama
    Bir kullanıcıyı doğrulamak için birden fazla doğrulama yönteminin kullanıldığı bir güvenlik sistemidir.

  - **NAC** : Ağ Erişim Kontrolü
    Bir ağ üzerindeki cihazların ve kullanıcıların kimlik doğrulaması yapılarak ağa erişimlerinin kontrol edildiği bir güvenlik teknolojisidir. NAC, sadece yetkili kullanıcıların ve cihazların ağa erişimini sağlar. Özellikle kurum ağında, NAC sistemi kullanarak sadece belirli kimlik bilgilerine sahip cihazların ağa bağlanmasına izin verilir.

  - **SIEM** : Güvenlik Bilgi ve Olay Yönetimi
    Güvenlik olaylarını ve verilerini toplamak, analiz etmek ve raporlamak için kullanılan bir sistemdir. SIEM, güvenlik tehditlerini hızlı bir şekilde tespit etmek ve yanıt vermek için kullanılır.

  - **Penetration Testing** : Sızma Testi
    Bir sistemin güvenlik açıklarını belirlemek ve bu açıkları kapatmak için yapılan simüle edilmiş siber saldırılardır. Testler, güvenlik uzmanları tarafından gerçekleştirilir ve sistemlerin ne kadar güvenli olduğunu değerlendirir.

- **Biyometrik Kimlik Doğrulama** :
  Kullanıcıların kimliklerini doğrulamak için parmak izi, iris taraması veya yüz tanıma gibi biyolojik özelliklerini kullanan bir güvenlik yöntemidir. Bu yöntemler, şifrelerin aksine daha güvenli ve kişiye özeldir.

- **Threat Intelligence** : Tehdit İstihbaratı
  Mevcut ve potansiyel siber tehditler hakkında bilgi toplama, analiz etme ve bu bilgileri kullanarak savunma stratejileri geliştirme sürecidir. Bu bilgi, saldırıların önceden tespit edilmesine ve etkili bir şekilde önlenmesine yardımcı olur. Örneğin, bir güvenlik firması, siber tehdit istihbaratı sağlayarak müşterilerini olası tehditlere karşı uyarır ve gerekli önlemleri almalarını sağlar.

- **Zero Trust** : Sıfır Güven
  Bir ağ veya sistemde varsayılan olarak hiçbir kullanıcıya veya cihaza güvenilmemesi anlamına gelir. Bu yaklaşım, her kullanıcının ve cihazın kimliğini doğrulayarak, erişim kontrolleri ve güvenlik politikaları uygulayarak herkesi sürekli olarak doğrulamayı ve izlemeyi amaçlar. Zero Trust modeli uygulanan bir ağda, iç ağda bulunan cihazlar bile her erişimde kimlik doğrulaması gerektirebilir.

- **SOAR** : Güvenlik Orkestrasyonu, Otomasyonu ve Müdahale
  Güvenlik olaylarına hızlı ve etkili bir şekilde yanıt vermek için otomasyon, orkestrasyon ve müdahaleyi entegre eden bir platform veya süreçler bütünüdür. Bu platformlar, güvenlik ekiplerinin olayları analiz etmesine, yanıtlamasına ve güvenlik olayları üzerinde otomatik veya yarı otomatik olarak işlem yapmasına olanak tanır.

- **Endpoint Security** : Uç Nokta Güvenliği
  Ağdaki her bir cihazın (bilgisayarlar, akıllı telefonlar, tabletler vb.) güvenliğini sağlamak için alınan tedbirlerdir. Uygulanan tedbirler, kötü amaçlı yazılımları engellemek, yetkisiz erişimleri önlemek ve uç nokta cihazlarının korunmasını sağlamak için kullanılır. Bir işletme, uç nokta güvenliği çözümleri kullanarak, çalışanların kullanıcı cihazlarında güvenlik açıklarını tespit eder ve açıkları kapatır, böylece ağ güvenliğini sağlar.