

Daphne Kariyer online eğitim · Dijital yetkinlikler · Siber güvenlik

Siber Güvenlik Temelleri

Modül	10
Önerilen süre	Yaklaşık 10–12 saat
Düzey	Başlangıç
Biçim	Online, kendi hızında
Ölçme	Daphne Kariyer ücretsiz testleri

İçindekiler

Modül 1 Bilgi güvenliğinin temeli

Modül 2 Tehdit türleri

Modül 3 Kimlik ve erişim yönetimi

Modül 4 Ağ güvenliğine giriş

Modül 5 Uç nokta ve e-posta güvenliği, güncelleme yönetimi

Modül 6 Yedekleme ve iş sürekliliği

Modül 7 Güvenlik izleme ve SOC'un işleyişi

Modül 8 Olay müdahalesi süreci

Modül 9 Etik hackerlık ve sızma testi

Modül 10 Standartlar, mevzuat ve güvenlik kültürü

Kendini dene cevapları · Sözlük · Sonraki adım

Bu eğitim hakkında

Bu eğitim iki gruba yönelik hazırlandı. Birinci grup, hangi bölümde çalışırsa çalışsın işini bilgisayar, telefon ve e-postayla yapan herkes: muhasebeciler, satış temsilcileri, insan kaynakları uzmanları, depo sorumluları, yöneticiler. İkinci grup, bilgi güvenliği alanında çalışmak isteyen ve sağlam bir başlangıç arayan kişiler. Önceden teknik bilgi gerekmez.

Eğitim savunma ve farkındalık odaklıdır. Saldırıların nasıl çalıştığını kavram düzeyinde anlatır ve her birinde nasıl korunacağını gösterir. Saldırı yapmayı öğreten adım adım talimat, araç komutu ya da istismar kodu yoktur. Güvenlik alanında çalışmak isteyenler için de doğru başlangıç noktası budur: önce neyi neden koruduğunu anlamak.

Eğitim 10 modülden oluşur: temel kavramlar ve tehditler, günlük korumalar (kimlik, ağ, uç nokta ve e-posta, yedekleme), izleme ve olay müdahalesi, etik hackerlık, son olarak standartlar ve mevzuat.

Her modülde gerçekçi iş örnekleri, bir uygulama ya da örnek vaka ve sık yapılan hatalar bölümü var. Her modülün sonunda beş soruluk "Kendini dene" bölümü bulunur; cevaplar eğitimin sonunda. Kitabın sonunda bir sözlük ve bilgini ölçebileceğin Daphne Kariyer testlerinin listesi yer alır. Eğitimi kendi hızında okursun; eğitmen ya da canlı ders yoktur.

Önerilen süre: yaklaşık 10–12 saat (okuma, örnekler, uygulamalar ve alıştırmalar dahil).

Eğitimin sonunda şunları yapabileceksin:

- Gizlilik, bütünlük ve erişilebilirlik ilkelerini açıklamak; risk, tehdit ve zafiyet arasındaki farkı örneklerle anlatmak.
- Zararlı yazılım, fidye yazılımı, oltalama, sosyal mühendislik ve DDoS gibi tehditleri tanımak ve her birine karşı temel önlemleri saymak.
- Güçlü parola, çok faktörlü kimlik doğrulama ve en az yetki ilkesini kendi işinde uygulamak.
- Güvenlik duvarı, ağ segmentasyonu, VPN ve kablosuz ağ güvenliğinin ne işe yaradığını anlatmak.
- Bilgisayar, telefon ve e-posta güvenliği için temel ayarları ve güncelleme düzenini kurmak.
- 3-2-1 yedekleme kuralını uygulamak; RPO ve RTO kavramlarıyla bir kurtarma hedefi belirlemek.
- Bir güvenlik operasyon merkezinin (SOC) logları, SIEM'i ve alarm triyajını nasıl kullandığını açıklamak.
- Olay müdahalesinin altı aşamasını sırasıyla anlatmak ve bir olay anında çalışan olarak ne yapman gerektiğini bilmek.
- Etik hackerlığı, sızma testini, yasal izin ve kapsam kavramlarını doğru yerde konumlandırmak.
- ISO/IEC 27001'in, 6698 sayılı KVKK'nın ve veri ihlali bildirimi yükümlülüğünün temel mantığını açıklamak.

Bilgi güvenliğinin temeli

Bir kurumun bilgisi müşteri listesi, maaş bordrosu, teklif dosyası, hasta kaydı gibi pek çok biçimde; sunucularda, bulutta, kâğıt üzerinde ya da çalışanların aklında bulunur. Bilgi güvenliği, bu bilginin nerede olursa olsun doğru kişilerce, doğru biçimde ve ihtiyaç duyulduğu anda kullanılabilmesini sağlamaktır.

Bilgi güvenliği ve siber güvenlik

İki terim günlük dilde çoğu zaman aynı anlamda kullanılır ama arada bir kapsam farkı vardır.

- **Bilgi güvenliği:** Bilginin her biçimini kapsar. Kilitli dolaptaki personel dosyaları, masada unutulan bir sözleşme, telefonda yüksek sesle söylenen bir parola da bu alanın konusudur.
- **Siber güvenlik:** Bilgisayarlar, ağlar, yazılımlar, bulut hizmetleri ve internete bağlı cihazlar üzerinden gelen tehditlere odaklanır. Bilgi güvenliğinin dijital ortamla ilgili büyük bir parçasıdır.

Bu eğitimde ağırlık siber güvenlikte; ama birçok saldırı bir insanı kandırarak başladığı için insan davranışı da konunun içinde.

Üç temel ilke: gizlilik, bütünlük, erişilebilirlik

Bilgi güvenliğinin bütün konuları üç ilkeye dayanır. İngilizce baş harfleriyle CIA üçlüsü (Confidentiality, Integrity, Availability) olarak da anılır.

- **Gizlilik:** Bilgiyi yalnız görmeye yetkili kişiler görebilir. Maaş bordrosunu yalnız insan kaynakları ve ilgili yöneticiler açabiliyorsa gizlilik korunuyordur. Bordro dosyası herkesin erişebildiği ortak klasöre konmuşsa gizlilik bozulmuştur.
- **Bütünlük:** Bilgi doğrudur, eksiksizdir ve izinsiz değiştirilmemiştir. Bir tedarikçinin banka hesap numarası sistemde sahte bir numarayla değiştirilirse, ödeme yanlış hesaba gider. Burada kimse bilgiyi çalmamıştır ama bütünlük bozulmuştur.
- **Erişilebilirlik:** Yetkili kişi bilgiye ve sisteme ihtiyaç duyduğu anda ulaşabilir. Bir e-ticaret sitesi kampanya gününde saatlerce açılmıyorsa, ya da bir hastanenin randevu sistemi fide yazılımı yüzünden kilitlenmişse erişilebilirlik bozulmuştur.

Bu üç ilke bazen birbirini zorlar. Hastanede acil servis hekiminin hasta kaydına hızla ulaşabilmesi erişilebilirlik açısından, aynı kaydın yalnız tedaviyle ilgili kişilerce görülmesi gizlilik açısından şarttır. Güvenlik çalışması, bu dengeyi işin ihtiyacına göre kurmaktır.

Bu üçlüye zaman zaman iki kavram daha eklenir. **Kimlik doğrulama**, bir işlemi yapanın gerçekten iddia ettiği kişi olduğunu kontrol etmektir. **İnkâr edilemezlik**, bir kişinin yaptığı bir işlemi sonradan "ben yapmadım" diye reddedememesidir. Elektronik imza ve düzgün tutulan işlem kayıtları bu ikinci kavrama hizmet eder.

Varlık, tehdit, zafiyet, risk

Güvenlik konuşmalarında dört kavram sürekli geçer. Birbirine karıştırılmaları en sık rastlanan kavram hatasıdır.

- **Varlık:** Kurum için değeri olan her şey. Müşteri veritabanı, muhasebe yazılımı, dizüstü bilgisayarlar, şirket web sitesi, kurumun itibarı ve çalışanların bilgisi birer varlıktır.
- **Tehdit:** Bir varlığa zarar verebilecek olası olay ya da kişi. Fidye yazılımı çetesi, dolandırıcı, sel, yangın, elektrik kesintisi, dikkatsiz bir çalışan birer tehdittir.
- **Zafiyet (açıklık):** Tehdidin yararlanabileceği zayıf nokta. Güncellenmemiş bir yazılım, "123456" parolası, yedeği olmayan bir sunucu, kapısı kilitsiz bir sunucu odası, ortalama e-postalarını tanımayan bir çalışan birer zafiyettir.
- **Risk:** Bir tehdidin bir zafiyeti kullanarak bir varlığa zarar verme ihtimali ve bu zararın büyüklüğü.

Bir örnekle bağlayalım. Ankara'da 15 kişilik bir muhasebe bürosu düşün. Varlık, müşterilerin beyanname ve bordro dosyalarıdır. Tehdit, bu dosyaları şifreleyip fidye isteyen bir saldırgandır. Zafiyet, büro sunucusunun aylardır güncellenmemiş olması ve yedeğin aynı sunucuda durmasıdır. Risk ise beyanname döneminde dosyaların erişilemez hâle gelmesi, müşterilerin cezalı duruma düşmesi ve büronun itibar kaybıdır.

Tehdidi çoğu zaman kontrol edemezsin; dünyada fidye yazılımı çeteleri var olmaya devam edecek. Kontrol edebildiğin şey zafiyetlerdir. Güvenlik çalışmasının büyük kısmı, zafiyetleri bulup kapatmak ve kapatılamayanların etkisini sınırlamaktır.

Riski değerlendirmek

Riskin büyüklüğü iki soruyla tahmin edilir: Bu olay ne kadar olası? Olursa etkisi ne kadar büyük olur? Basit bir yaklaşımda her biri 1 ile 5 arasında puanlanır ve iki puan çarpılır.

- **Olasılık:** 1 çok düşük, 5 neredeyse kesin.
- **Etki:** 1 önemsiz, 5 işi durduran ya da ciddi yasal sonuç doğuran.
- **Risk puanı:** Olasılık çarpı etki. 1 ile 25 arasında bir değer çıkar.

Muhasebe bürosu örneğinde "güncellenmemiş sunucu yüzünden fidye yazılımı bulaşması" için olasılık 4, etki 5 verilebilir; risk puanı 20 olur. "Sunucu odasına su basması" için olasılık 1, etki 4 verilirse puan 4 olur. Bu basit hesap, sınırlı bütçeyi önce nereye harcayacağını gösterir.

Puanlar kesin değerler değil, ekibin ortak değerlendirmesidir. Önemli olan aynı ölçeği tutarlı kullanmak ve her puanın gerekçesini bir cümleyle yazmaktır.

Riske karşı dört seçenek

Bir risk belirlendikten sonra dört yoldan biri seçilir.

1. **Azaltmak:** Bir önlem alarak olasılığı ya da etkiyi düşürmek. Sunucuyu güncellemek ve yedeği ayrı bir yerde tutmak bu yoldur. En sık kullanılan seçenektir.
2. **Aktarmak:** Riskin mali sonucunu başkasına devretmek. Siber sigorta yaptırmak ya da bir hizmeti sözleşmeyle uzman bir sağlayıcıya vermek bu yoldur. Dikkat: sorumluluk tamamen aktarılmaz. Müşteri verisi sızarsa yasal sorumluluk çoğunlukla yine kurumda kalır.
3. **Kaçınmak:** Riski doğuran işi hiç yapmamak. Kredi kartı bilgisini kendi sisteminde saklamak yerine hiç saklamamak ve ödemeyi bir ödeme kuruluşuna bırakmak bu yoldur.
4. **Kabul etmek:** Önlemin maliyeti riskten büyükse, riski bilerek üstlenmek. Bu karar yetkili bir yönetici tarafından verilir ve yazılı kayıt altına alınır. "Kimse fark etmedi, öyle kaldı" kabul değil ihmaldir.

Güvenlik kontrolleri

Riski azaltmak için alınan her önleme **kontrol** denir. Kontroller iki şekilde gruplanabilir.

İşlevine göre:

- **Önleyici:** Olayın olmasını engeller. Çok faktörlü kimlik doğrulama, güvenlik duvarı kuralı, kilitli kapı.
- **Tespit edici:** Olay olduğunda fark edilmesini sağlar. Güvenlik kamerası, log izleme, alarm sistemi.
- **Düzeltilici:** Olaydan sonra durumu düzeltir. Yedekten geri yükleme, ele geçirilmiş hesabın parolasını sıfırlama.

Niteliğine göre:

- **İdari:** Politika, prosedür, eğitim, görev tanımı. "Tedarikçi banka hesabı değişikliği telefonla teyit edilmeden yapılmaz" kuralı idari bir kontroldür.
- **Teknik:** Yazılım ve donanımla uygulanan önlemler. Şifreleme, antivirüs, erişim yetkileri.
- **Fiziksel:** Mekâna ve cihaza yönelik önlemler. Kartlı geçiş, kilitli dolap, sunucu odasında yangın söndürme sistemi.

Hiçbir önleyici kontrol kusursuz olmadığı için, ters giden bir şeyi fark edecek ve düzeltecek kontroller de gerekir.

Derinlemesine savunma

Eski kalelerde surun önünde hendek, surun içinde ikinci bir duvar, en içte de korunaklı bir kule bulunurdu. Saldırgan bir engeli aşsa bile karşısına bir başkası çıkardı. Bilgi güvenliğinde buna **derinlemesine savunma** (defense in depth) denir.

Bir oltalama e-postası düşün. E-posta filtresi onu yakalayamadı. Çalışan bağlantıya tıkladı ve parolasını sahte sayfaya yazdı. Ama hesapta çok faktörlü doğrulama açık olduğu için saldırgan giriş yapamadı. Diyelim ki o da aşıldı; bu kez çalışanın yetkileri sınırlı olduğu için saldırgan kritik sistemlere ulaşamadı. Bu da aşıldıysa, izleme sistemi olağandışı girişi fark edip alarm üretti. Her katman tek başına yetersizdir, birlikte güçlüdür.

İnsan, süreç, teknoloji

Güvenlik yalnız teknoloji satın alarak sağlanmaz. Üç ayağı vardır:

- **İnsan:** Çalışanların farkındalığı, sorumluluk bilinci ve şüpheli durumu bildirme alışkanlığı.
- **Süreç:** İşlerin nasıl yapılacağını tanımlayan kurallar. İşe giriş ve çıkışta hesap açma ve kapatma, ödeme onayı, yedekleme takvimi.
- **Teknoloji:** Bu süreçleri destekleyen araçlar.

Alarmlarına kimsenin bakmadığı pahalı bir ürün de, çalışanların bilmediği iyi yazılmış bir politika da işe yaramaz.

Örnek vaka: muhasebe bürosunun ilk risk listesi

Ankara'daki 15 kişilik muhasebe bürosunun ortağı, bir meslektaşının bürosunun fidye yazılımına yakalandığını duyunca bir risk listesi hazırlamaya karar verir. Teknik bir uzmanı yoktur; büronun bilgi işlerine yarı zamanlı bakan dış destek firmasıyla bir öğleden sonra oturur.

1. Önce varlıkları listelerler: müşteri dosyalarının durduğu sunucu, muhasebe yazılımı, e-posta hesapları, 15 dizüstü bilgisayar, e-imza ve mali mühür cihazları, kâğıt arşiv.
2. Her varlık için başına ne gelebileceğini konuşurlar: şifrelenme, çalınma, kaybolma, yanlış kişiye gönderilme, yangın.
3. Mevcut zafiyetleri yazarlar: sunucu güncellemeleri düzensiz, yedek aynı sunucuda bir klasörde, herkes aynı ortak parolayla sunucuya bağlanıyor, e-postalarda ikinci doğrulama yok.
4. Her risk için olasılık ve etki puanı verirler. En yüksek puanları fidye yazılımı (20) ve e-posta hesabının ele geçirilmesi (16) alır.
5. İlk üç ay için üç önlem seçerler: yedeği bürodan ayrı ve bağlantısız bir ortama almak, kişisel kullanıcı hesaplarına geçmek, e-postada çok faktörlü doğrulamayı açmak.
6. Kâğıt arşivin yangın riskini, düşük olasılık nedeniyle şimdilik kabul eder ve bunu tarihli bir notla kayda geçirirler.

Liste mükemmel değildir ama büro ilk kez neyi neden koruduğunu görür. Üç ay sonra liste yeniden gözden geçirilir.

Sık yapılan hatalar

- **Güvenliği yalnız bilgi işlemin işi saymak.** Oltalama e-postasına tıklayan, ödeme talimatını teyit etmeden uygulayan, parolasını paylaşan kişi çoğu zaman teknik bölümden değildir.
- **Tehdit ile zafiyeti karıştırmak.** "Riskimiz hackerlar" demek riski tanımlamaz. Hangi varlık, hangi zafiyet ve olursa ne olacağı yazılmadıkça önlem seçilemez.
- **"Bizde çalınacak bir şey yok" düşüncesi.** Küçük işletmeler de hedef olur. Saldırganların büyük kısmı fırsatçıdır; belirli bir kurumu değil, açığı olan herhangi bir sistemi arar. Ayrıca fidye yazılımında amaç veriyi çalmak değil, işi durdurup para istemektir.
- **Tek bir ürüne güvenmek.** "Antivirüsümüz var" ya da "güvenlik duvarımız var" cümlesi tek katmanlı bir savunmayı anlatır.
- **Kabul edilen riskleri yazmamak.** Kimin, neden, hangi tarihte riski kabul ettiği belli değilse, bu bir karar değil unutkanlıktır.
- **Risk listesini bir kez yapıp rafa kaldırmak.** Kurum, sistemler ve tehditler değişir. Liste en az yılda bir, büyük değişikliklerden sonra da yeniden gözden geçirilmelidir.

Kendini dene

1. Bir tedarikçinin banka hesap numarasının sistemde izinsiz değiştirilmesi hangi temel ilkeyi bozar?
2. "Güncellenmemiş yazılım" bir tehdit midir, zafiyet midir?
3. Olasılığı 3, etkisi 4 olan bir riskin puanı basit çarpım yöntemine göre kaçtır?
4. Siber sigorta yaptırmak dört risk seçeneğinden hangisine örnektir?
5. Derinlemesine savunma ne demektir? Bir cümleyle açıkla.

Tehdit türleri

Bu modülde iş hayatında en sık karşılaşılan tehditleri tanıyacaksınız. Amaç saldırı tekniği öğrenmek değil, belirtileri fark etmek ve doğru önlemleri seçmektir.

Saldırganlar kimdir, ne ister?

Saldırganlar tek tip değildir. Amaçlarını bilmek, hangi tehdidin seni daha çok ilgilendirdiğini anlamaya yardımcı eder.

- **Para peşindeki suç grupları:** En yaygın gruptur. Fidyeye yazılımı, kart bilgisi hırsızlığı, sahte fatura ve ödeme dolandırıcılığı yaparlar. Çoğu fırsatçıdır; açığı olan herhangi bir kurumu hedef alır.
- **İç tehdit:** Kurumun kendi çalışanı, eski çalışanı ya da erişimi olan bir tedarikçi. Kasıtlı olabilir (işten ayrılırken müşteri listesini götürmek) ya da kasıtsız (yanlış kişiye dosya göndermek, parolayı paylaşmak). Kasıtsız iç tehdit, kasıtlı olandan çok daha sık görülür.
- **Hacktivistler:** Siyasi ya da toplumsal bir mesaj vermek için web sitelerini tahrip eden ya da erişilemez hâle getiren gruplar.
- **Devlet destekli gruplar:** Casusluk ya da kritik altyapıya zarar verme amaçlı, uzun süre fark edilmeden kalmayı hedefleyen gruplar.

Zararlı yazılım türleri

Zararlı yazılım (malware), sahibinin izni olmadan bir cihazda zarar verici iş yapan her türlü yazılımın genel adıdır. Başlıca türleri şunlardır:

- **Virüs:** Başka bir dosyaya ya da programa eklenerek yayılır; o dosya çalıştırıldığında etkinleşir.
- **Solucan (worm):** Kullanıcı bir şey yapmadan, ağdaki güncellenmemiş sistemlere kendi kendine yayılır. Bir ağda çok hızlı çoğalabilir.
- **Truva atı (trojan):** Faydalı bir program gibi görünür, arka planda başka iş yapar. Korsan bir ofis programı ya da "ücretsiz PDF dönüştürücü" kılığında gelebilir.
- **Casus yazılım (spyware) ve tuş kaydedici (keylogger):** Kullanıcının yaptıklarını, yazdığı parolaları ve ekranını gizlice kaydedip saldırganlara iletir.
- **Uzaktan erişim aracı:** Saldırganın cihazı uzaktan yönetmesini sağlar. Meşru uzaktan destek programları da saldırganlar tarafından kötüye kullanılabilir.
- **Bot ve botnet:** Ele geçirilmiş cihazlara bot, bunların bir merkezden yönetilen ağına botnet denir. Botnetler spam göndermek ve DDoS saldırısı yapmak için kullanılır. Güvenliği zayıf kameralar ve modemler de botnete katılabilir.
- **Kripto para madencisi:** Cihazın işlemci gücünü saldırgan adına kripto para üretmek için kullanır. Belirtisi, cihazın sebepsiz yavaşlaması ve fanının sürekli çalışmasıdır.

Zararlı yazılımlar çoğunlukla şu yollardan gelir: e-posta eki ya da bağlantısı, sahte ya da korsan yazılım indirme, güncellenmemiş yazılımdaki açıklar, ele geçirilmiş web siteleri ve bulunup takılan USB bellekler.

Fidye yazılımı

Fidye yazılımı (ransomware) bugün kurumlar için en yıkıcı tehditlerden biridir. Saldırgan kurumun dosyalarını ve sistemlerini şifreler, çözmek için fidye ister. Ödeme genellikle kripto para ile talep edilir.

Bugünkü saldırılar çoğunlukla aşamalıdır. Saldırgan çalınmış bir parola, güncellenmemiş bir VPN cihazı ya da ortalama e-postasıyla içeri girer, ağda günlerce dolaşır, yedekleri siler, verileri dışarı kopyalar ve şifrelemeyi çoğunlukla gece ya da hafta sonu başlatır.

Buna **çifte şantaj** denir: saldırgan hem dosyaları şifreler hem de dışarı çıkardığı veriyi yayımlamakla tehdit eder. Yani yedekten geri dönmek işi kurtarır ama veri sızıntısı sorununu çözmez.

Fidye ödemek bir çözüm garantisi değildir. Şifre çözücü hiç gelmeyebilir, gelen araç düzgün çalışmayabilir, çalınan veri yine yayımlanabilir ve ödeme yapan kurum ileride yeniden hedef olabilir. Bu karar hukuki boyutları olan bir yönetim kararıdır; tek başına bir çalışanın ya da bilgi işlem sorumlusunun vereceği bir karar değildir.

Fidye yazılımına karşı en etkili önlemler bu eğitimin sonraki modüllerinde tek tek anlatılıyor: çok faktörlü doğrulama, güncel sistemler, en az yetki, ağ segmentasyonu, izleme ve en önemlisi saldırganın erişemeyeceği yedekler.

Oltalama

Oltalama (phishing), kişiyi sahte bir mesajla kandırarak parola, kart bilgisi gibi bilgileri vermesini, bir dosyayı açmasını ya da para göndermesini sağlama girişimidir. Saldırıların çok büyük bir kısmı bir oltalama mesajıyla başlar.

Oltalamanın türleri:

- **E-posta oltalaması:** Kargo şirketi, banka, vergi dairesi, bulut depolama hizmeti ya da kurumun kendi bilgi işlem bölümü taklit edilir.
- **SMS oltalaması (smishing):** "Gönderiniz adres eksikliği nedeniyle bekletiliyor" gibi kısa mesajlar.
- **Sesli oltalama (vishing):** Telefonla banka görevlisi, savcı, polis ya da şirketin bilgi işlem destek ekibi taklit edilir.
- **Hedefli oltalama (spear phishing):** Belirli bir kişiye, onun işini ve çevresini bilerek hazırlanmış mesaj. Örneğin satın alma uzmanına, gerçekten çalıştığı bir tedarikçinin adıyla gönderilen sahte fatura.
- **Üst yönetici oltalaması (whaling):** Genel müdür, finans müdürü gibi yüksek yetkili kişileri hedefleyen oltalama.
- **QR kod oltalaması:** Bağlantı yerine QR kod içeren e-posta ya da afiş. Kod, telefonda açıldığı için kurumsal filtrelerin dışında kalabilir.

Oltalama mesajlarında sık görülen işaretler:

1. **Aciliyet ve baskı:** "24 saat içinde doğrulamazsanız hesabınız kapatılacak."
2. **Gönderen adresinde tutarsızlık:** Görünen ad bankanın adı ama adres alakasız bir alan adı; ya da kurum adında bir harf değişikliği.
3. **Beklenmeyen ek ya da bağlantı:** Sipariş vermediğin bir faturanın eki, katılmadığın bir toplantının belgesi.

4. **Bağlantının gittiği yer:** Bağlantının üzerine tıklamadan gelince görünen adres, mesajdaki kurumla eşleşmiyor.
5. **Olağan dışı talep:** Parola, kart bilgisi, doğrulama kodu ya da acil ödeme istemek.

Yapay zekâ araçları sayesinde artık kusursuz Türkçeyle yazılmış ortalama mesajları da geliyor; dil kalitesine değil, talebin kendisine bak.

Sosyal mühendislik

Sosyal mühendislik, teknik bir açık yerine insanların güvenini, yardımseverliğini, merakını ya da korkusunu kullanmaktır. Ortalama bunun en yaygın biçimidir ama tek biçimi değildir.

- **Bahane uydurma (pretexting):** Saldırgan inandırıcı bir hikâye kurar. "Merhaba, ben yeni başlayan bilgi işlem stajyeriyim, sistem geçişi için kullanıcı adınızı ve size gelen kodu okur musunuz?"
- **Kuyruk takibi (tailgating):** Kartlı kapıdan girerken arkanızdan elinde kolilerle gelen kişiye kapıyı tutmak. Kibarlık, yetkisiz girişe dönüşebilir.
- **Yem bırakma (baiting):** Otoparka ya da bekleme salonuna "Maaşlar 2026" etiketli bir USB bellek bırakmak. Merak eden kişi onu bilgisayarına takar.
- **Karşılıklık ve iyilik:** Önce küçük bir yardım ya da hediye sunup sonra bilgi istemek.

Sosyal mühendisliğe karşı en etkili önlem, belirli talepler için **ikinci bir kanaldan teyit** kuralıdır. Parola, doğrulama kodu ya da ödeme bilgisi isteyen herhangi bir talebi, sana ulaşılan kanal yerine önceden bilinen bir kanaldan doğrula. Telefon numarasını mesajdan değil, kurumun rehberinden ya da resmî sitesinden al.

İş e-postası dolandırıcılığı

İş e-postası dolandırıcılığı (Business Email Compromise, BEC), zararlı yazılım bile gerektirmeyen ama çok büyük paralar kaybettirebilen bir saldırdır. İki yaygın biçimi vardır:

- **Sahte yönetici talimatı:** Finans çalışanına genel müdür adına, "gizli bir satın alma için bugün şu hesaba ödeme yapılması gerekiyor, kimseyle paylaşma" diye yazılır.
- **Tedarikçi hesap değişikliği:** Gerçek bir tedarikçinin ele geçirilmiş ya da taklit edilmiş e-posta hesabından, "banka hesabımız değişti, bundan sonraki ödemeleri yeni hesaba yapınız" mesajı gelir.

Buradaki önlem teknik olmaktan çok süreçle ilgilidir: banka hesabı değişikliği ve olağan dışı ödemeler, kayıtlı bir telefon numarasından sesli teyit ve iki kişilik onay olmadan uygulanmaz.

DDoS kavramı

Dağıtık hizmet engelleme saldırısı (Distributed Denial of Service, DDoS), çok sayıda cihazdan bir sisteme aynı anda yoğun trafik ya da istek göndererek onu gerçek kullanıcılara hizmet veremez hâle getirmektir. Bir mağazanın kapısına yüzlerce kişinin aynı anda yığılması ve gerçek müşterinin içeri girememesi gibi düşünebilirsiniz.

DDoS erişilebilirliği hedefler, çoğunlukla veri çalmaz; bazen başka bir saldırıdan dikkati dağıtmak için kullanılır. Kurumlar genellikle internet servis sağlayıcılarının ya da içerik dağıtım ağı (CDN) hizmetlerinin DDoS korumasından yararlanır; kampanya dönemi olan bir e-ticaret sitesi bunu önceden planlamalıdır.

Tedarik zinciri saldırıları

Saldırgan bazen doğrudan hedefe değil, ona hizmet veren bir firmaya saldırır: muhasebe yazılımı sağlayıcısı, uzaktan destek veren bilgi işlem firması, yazılım güncellemelerini dağıtan bir şirket. Bu firmalar üzerinden onlarca müşteriye ulaşabilir. Bu yüzden tedarikçilere verilen erişimler de sınırlı, kayıtlı ve izlenir olmalıdır.

Örnek vaka: e-ticaret mağazasına gelen kargo mesajı

Bursa'da ev tekstili satan 12 kişilik bir e-ticaret mağazasında müşteri hizmetleri çalışanı bir sabah şu e-postayı alır: gönderen adı anlaşmalı kargo firmasının adıdır, konu "Teslim edilemeyen gönderi faturası". Ekte "fatura" adlı sıkıştırılmış bir dosya vardır ve mesaj, gönderinin iadesini önlemek için faturanın bugün onaylanması gerektiğini söyler.

Çalışan şu kontrolleri yapar:

1. Gönderen adresine bakar; kargo firmasının alan adı değil, alakasız bir adres.
2. Mağazanın kargo firmasıyla bütün yazışmaları zaten firma panelinden yürüdüğü için e-posta ile fatura gelmesi olağan dışıdır.
3. Eki açmaz, bağlantıya tıklamaz.
4. Kurumun belirlediği yoldan, e-postayı "şüpheli" olarak bilgi işlem sorumlusuna bildirir.
5. Kargo panelinden ilgili gönderiyi kontrol eder; böyle bir sorun yoktur.

Sorumlu, aynı e-postanın üç çalışana daha geldiğini görür ve hepsini posta kutularından kaldırır.

Sık yapılan hatalar

- **Yalnız dil hatalarına bakmak.** Kusursuz yazılmış bir mesaj da sahte olabilir. Asıl soru: bu talep olağan mı, beklediğim bir şey mi?
- **Mesajdaki telefon numarasını arayarak teyit etmek.** Saldırganın verdiği numarayı aramak, yine saldırganla konuşmak demektir.
- **Tıkladıktan sonra utanıp sessiz kalmak.** Erken bildirim, hasarı sınırlamanın en ucuz yoludur. İyi bir kurum bildirimini cezalandırmaz.
- **"Ödersek kurtuluruz" varsayımı.** Fidyeye ödemesi verinin geri geleceğini ya da yayımlanmayacağını garanti etmez.
- **Bulunan USB belleği "sahibini bulmak için" takmak.** Bilinmeyen bellek, bilgi işleme teslim edilir.
- **Kapıyı nezaketen tutup kimliğe bakmamak.** Kartsız birini içeri almak yerine onu resepsiyona yönlendirmek kaba değil, doğrudur.

Kendini dene

1. Kullanıcı bir şey yapmadan ağdaki sistemlere kendi kendine yayılan zararlı yazılım türüne ne ad verilir?
2. Çifte şantaj içeren fidye yazılımı saldırısında yedekten geri dönmek hangi sorunu çözmez?
3. Telefonla yapılan oltalama girişimine ne ad verilir?
4. Tedarikçiden "banka hesabımız değişti" e-postası geldiğinde ilk yapman gereken nedir?
5. DDoS saldırısı gizlilik, bütünlük ve erişilebilirlikten hangisini doğrudan hedefler?

Kimlik ve erişim yönetimi

Saldırganlar çoğu zaman sistemleri "kırarak" değil, geçerli bir kullanıcı adı ve parolayla oturum açarak içeri girer. Bu yüzden kimin hangi sisteme nasıl girdiğini ve içeride neler yapabildiğini yönetmek, güvenliğin en temel işlerinden biridir. Bu alana kimlik ve erişim yönetimi (Identity and Access Management, IAM) denir.

Kimlik, kimlik doğrulama, yetkilendirme

Üç kavram birbirine yakındır ama farklı soruları cevaplar.

- **Kimlik:** Sen kimsin? Kullanıcı adı, personel numarası ya da e-posta adresi bir kimliği temsil eder.
- **Kimlik doğrulama (authentication):** Gerçekten o kişi misin? Parola, telefona gelen onay ya da parmak izi bunu kanıtlamaya yarar.
- **Yetkilendirme (authorization):** İçeri girdikten sonra neleri yapabilirsin? Satış temsilcisi müşteri kartlarını görebilir ama maaş bilgilerini göremez.

Bunlara **kayıt tutma** eklenir: kimin ne zaman hangi sisteme girdiği ve ne yaptığı kaydedilir.

Parolalar

Parola hâlâ en yaygın kimlik doğrulama yöntemidir ve en çok saldırıya uğrayan noktadır. Parolalar genellikle üç yoldan ele geçirilir: ortalama sayfasına yazdırılarak, başka bir sitede sızan parolanın denenmesiyle ve tahmin edilmesi kolay parolaların denenmesiyle.

İkinci yol özellikle önemlidir. Bir alışveriş sitesinden sızan e-posta ve parola çiftleri, saldırganlar tarafından otomatik olarak e-posta servislerinde, bankalarda ve kurumsal sistemlerde denir. Buna **kimlik bilgisi doldurma** (credential stuffing) denir. Aynı parolayı birden fazla yerde kullanan kişi, en zayıf sitenin güvenliğine bağlı kalır.

İyi bir parola için temel kurallar:

- **Uzunluk karmaşıklıkla önemlidir.** "Ys#8k" gibi kısa ve karmaşık bir parola yerine, birbiriyle ilgisiz dört beş kelimeden oluşan uzun bir parola cümlesi hem daha güçlü hem daha kolay hatırlanır. Kurumlar genellikle en az 12 karakter ister; daha uzun daha iyidir.
- **Her hesap için farklı parola.** Özellikle kurumsal e-posta parolası başka hiçbir yerde kullanılmamalıdır.
- **Kişisel bilgi yok.** Doğum yılı, takım adı, çocuğun adı, şirket adı ve yıl ("Firma2026") ilk denenecek tahminler arasındadır.
- **Parola yöneticisi kullan.** Onlarca farklı ve uzun parolayı akılda tutmak mümkün değildir. Kurumun onayladığı bir parola yöneticisi bu parolaları şifreli bir kasada saklar; sen yalnız tek bir güçlü ana parolayı hatırlarsın.
- **Paylaşma.** Parola telefonla, e-postayla ya da ekip sohbetinde paylaşılmaz. Bilgi işlem ekibi senden parolanı istemez; isteyen biri varsa bu bir uyarı işaretidir.

Eskiden yaygın olan "her 90 günde parolanı değiştir" kuralı artık birçok güncel rehberde önerilmiyor. Sık zorunlu değişiklik, insanları "Parola1, Parola2" gibi tahmin edilebilir dizilere itiyor. Bunun yerine parola ancak sızdığından ya da ele geçirildiğinden şüphelenildiğinde değiştirilir; buna karşılık uzunluk ve tekillik şartı sıkı tutulur. Kurumunun kuralı farklıysa, kurumunun kuralına uy.

Çok faktörlü kimlik doğrulama

Çok faktörlü kimlik doğrulama (Multi-Factor Authentication, MFA), oturum açarken birbirinden farklı türde en az iki kanıt istemektir. Faktör türleri üçtür:

- **Bildiğin bir şey:** Parola, PIN.
- **Sahip olduğun bir şey:** Telefon, donanım güvenlik anahtarı, akıllı kart.
- **Olduğun bir şey:** Parmak izi, yüz tanıma.

İki parola istemek MFA değildir, çünkü ikisi de aynı türdendir. MFA'nın gücü şuradan gelir: saldırgan parolanı ele geçirirse bile, telefonun ya da anahtarın elinde olmadığı için giriş yapamaz.

MFA yöntemleri güç açısından aynı değildir:

- **SMS ile gelen kod:** Hiç olmamasından çok daha iyidir. Ancak SIM kart değiştirme dolandırıcılığına ve kodun sahte sayfaya yazdırılmasına açıktır.
- **Doğrulama uygulaması:** Telefondaki bir uygulamanın ürettiği, kısa sürede değişen kodlar ya da "onayla / reddet" bildirimleri. SMS'ten güçlüdür.
- **Donanım güvenlik anahtarı ve geçiş anahtarı (passkey):** Oltalamaya en dayanıklı yöntemlerdir. Anahtar yalnız gerçek siteyle çalışır; sahte bir sayfaya kod yazdırılamaz. FIDO2 standardına dayanırlar.

Bilmen gereken bir saldırı türü **MFA yorgunluğu**dur. Parolanı ele geçiren saldırgan, telefonuna art arda onay bildirimi gönderir ve bir an dikkatsizlikle ya da bıkkınlıkla "onayla"ya basmanı umar. Kural basittir: oturum açmaya çalışmadığın bir anda gelen onay isteğini asla onaylama, reddet ve bilgi işleme bildir. Beklenmedik bir onay isteği, parolanın başkasının elinde olduğu anlamına gelir; parolanı hemen değiştir.

MFA'nın öncelikle açılması gereken yerler: e-posta, uzaktan erişim (VPN), bulut hizmetleri, yönetici hesapları, muhasebe ve bankacılık sistemleri.

En az yetki ilkesi

En az yetki ilkesi (least privilege), her kullanıcıya ve her sisteme işini yapması için gereken en az erişimin verilmesidir. Ne eksik ne fazla.

Bir hastanede danışmadaki görevli randevu bilgisini görür ama tahlil sonuçlarını görmez. Laboratuvar teknisyeni tahlil sonucunu girer ama faturalama ekranına giremez. Böylece bir hesap ele geçirilirse ya da bir çalışan hata yaparsa, zarar o hesabın yetki alanıyla sınırlı kalır.

En az yetkiye yakın bir kavram da **görevlerin ayrılığıdır**. Kritik bir işin tamamı tek bir kişiye bırakılmaz. Ödemeyi hazırlayan kişi ile onaylayan kişinin farklı olması, hem hatayı hem kötüye kullanımı zorlaştırır.

Yetkiler kişi kişi değil **rol** bazında verildiğinde yönetim kolaylaşır. "Satış temsilcisi", "depo sorumlusu", "muhasebe uzmanı" gibi roller tanımlanır, her rolün yetkisi bir kez belirlenir, kişiler rollere atanır. Buna rol tabanlı erişim denetimi (Role-Based Access Control, RBAC) denir.

Ayrıcalıklı hesaplar

Sistem yöneticisi, veritabanı yöneticisi ya da etki alanı yöneticisi gibi geniş yetkili hesaplara **ayrıcalıklı hesap** denir. Saldırganların en çok aradığı hesaplar bunlardır, çünkü bir ayrıcalıklı hesapla bütün ağı kontrol edebilirler.

Temel kurallar:

- Yönetici yetkisi olan kişi, günlük işleri (e-posta okumak, internette gezinmek) için ayrı ve yetkisiz bir hesap kullanır. Yönetici hesabı yalnız yönetim işi için açılır.
- Çalışanların kendi bilgisayarlarında yerel yönetici yetkisi olmaz. Program kurulumu bilgi işlem üzerinden yapılır.
- Ayrıcalıklı hesaplarda MFA zorunludur.
- Ortak kullanılan yönetici hesapları ("admin" hesabını üç kişinin bilmesi) yerine kişiye özel hesaplar kullanılır, böylece kimin ne yaptığı kayıtlardan anlaşılır.
- Büyük kurumlarda ayrıcalıklı erişim yönetimi (Privileged Access Management, PAM) araçlarıyla bu hesapların parolaları kasada tutulur, oturumlar kaydedilir ve yetki yalnız gerektiği süre için verilir.

Hesap yaşam döngüsü

Erişim yönetimi, bir çalışanın kuruma girişinden ayrılışına kadar süren bir süreçtir.

1. **İşe girişi:** Rolüne uygun hesaplar açılır. Yöneticinin yazılı talebi olmadan hesap açılmaz.
2. **Görev değişikliği:** Satıştan satın almaya geçen çalışanın yeni rolün yetkileri verilirken eski rolün yetkileri de kaldırılır. Bu adım en sık unutulmuş adımdır; yıllar içinde yetki biriken kişilere sık rastlanır.
3. **İşten ayrılışı:** Son iş gününde bütün hesaplar kapatılır ya da devre dışı bırakılır; uzaktan erişim, e-posta, bulut hizmetleri ve kartlı geçiş dahil. Zimmetli cihazlar geri alınır.

İnsan kaynakları ile bilgi işlem arasında bu olayları bildiren net bir süreç yoksa sahipsiz ama açık hesaplar birikir. Kimse kullanmadığı için bu hesaplardaki olağan dışı hareketi de kimse fark etmez.

Tek oturum açma

Tek oturum açma (Single Sign-On, SSO), kullanıcının tek bir kurumsal kimlikle birçok uygulamaya girmesini sağlar. Kullanıcı için kolaylık, güvenlik için merkezi kontrol demektir: MFA tek bir yerde uygulanır, işten ayrılan kişinin tek hesabı kapatılınca bütün uygulamalara erişimi kesilir. Karşılığında bu merkezi hesabın çok iyi korunması gerekir.

Uygulama: üç aylık erişim gözden geçirmesi

İzmir'de 40 kişilik bir lojistik firması, her üç ayda bir erişim gözden geçirmesi yapmaya karar verir. Süreç şöyle işler:

1. Bilgi işlem sorumlusu, kritik sistemlerdeki (muhasabe yazılımı, depo yönetim sistemi, e-posta, dosya sunucusu, araç takip paneli) kullanıcı ve yetki listelerini dışa aktarır.
2. Liste, insan kaynaklarının güncel personel listesiyle karşılaştırılır. Personel listesinde olmayan her hesap işaretlenir.

3. Her bölüm yöneticisine kendi ekibinin yetki listesi gönderilir. Yönetici her satır için "kalsın", "kaldırılsın" ya da "değişsin" yazar.
4. Yönetici hesapları ayrıca incelenir: kaç tane var, kimde, MFA açık mı?
5. Son 90 günde hiç kullanılmamış hesaplar devre dışı bırakılır.
6. Yapılan değişiklikler ve yöneticilerin onayları tarihli bir kayıta saklanır.

İlk gözden geçirmede firma, iki yıl önce ayrılmış bir sevkiyat uzmanının araç takip panelinde hâlâ açık hesabı olduğunu, muhasebe yazılımında beş kişinin yönetici yetkisi taşıdığını ve depo sisteminde herkesin aynı ortak kullanıcıyla çalıştığını fark eder. Bu üç bulgu, sonraki üç ayın iş listesi olur.

Sık yapılan hatalar

- **Aynı parolayı iş ve kişisel hesaplarda kullanmak.** Kişisel bir sitedeki sızıntı, kurumsal hesabın kapısını açar.
- **MFA'yı yalnız yöneticilere açmak.** Saldırganlar çoğu zaman sıradan bir çalışanın hesabıyla başlar, sonra yetki toplar.
- **Beklenmedik MFA onayına "yanlışlıkla gelmiştir" diyerek basmak.** Beklenmedik istek, saldırının kendisidir.
- **"Ne olur ne olmaz" diye fazla yetki vermek.** Fazla yetki, ele geçirilen hesabın zararını büyütür.
- **Ortak hesaplar.** "depo1" gibi herkesin bildiği hesaplarla kimin ne yaptığı anlaşılamaz ve parola hiçbir zaman değiştirilemez.
- **İşten ayrılan kişinin hesabını açık bırakmak.** Özellikle bulut hizmetleri ve uzaktan erişim hesapları unutulur.
- **Parolayı ekran kenarına yapışkan notla yazmak.** Fiziksel güvenliği zayıf bir ofiste bu, parolayı herkese vermektir.

Kendini dene

1. Kimlik doğrulama ile yetkilendirme arasındaki fark nedir?
2. Başka bir siteden sızan parolaların otomatik olarak farklı sistemlerde denenmesine ne ad verilir?
3. Parola ve PIN kodu istemek neden çok faktörlü kimlik doğrulama sayılmaz?
4. Oturum açmaya çalışmadığın bir anda telefonuna onay bildirimi gelirse ne yapmalısın?
5. Görev değişikliğinde erişim yönetimi açısından en sık unutilan adım nedir?

Ağ güvenliğine giriş

Kurumdaki bilgisayarlar, sunucular, yazıcılar, kameralar ve telefonlar bir ağ üzerinden birbirine ve internete bağlanır. Ağ, saldırganın içeri girdiği ve içeride dolaştığı yoldur. Ağ güvenliği, bu yolları kontrol altına almaktır: kim nereye bağlanabilir, hangi trafik serbest, hangisi yasak?

Birkaç temel kavram

- **IP adresi:** Ağdaki her cihazın adresi. Bir binanın sokak adresine benzer.
- **Port:** Bir cihazdaki belirli bir hizmetin kapısı. Aynı sunucu bir porttan web sayfası, başka bir porttan e-posta hizmeti verebilir. Binadaki daire numaraları gibi düşünebilirsiniz.
- **Protokol:** Cihazların birbiriyle hangi kurallarla konuşacağını belirleyen ortak dil. Web için HTTP ve onun şifreli hâli HTTPS, e-posta için SMTP gibi.
- **Yerel ağ (LAN) ve geniş alan ağı (WAN):** Yerel ağ ofisin içindeki ağıdır. Geniş alan ağı, şubeleri ya da ofisi internete bağlayan dış bağlantıdır.

Saldırganın ilk işlerinden biri, internete açık hangi cihazların ve hangi portların bulunduğunu öğrenmektir. İnternete açık her gereksiz hizmet, saldırı yüzeyini büyütür. **Saldırı yüzeyi**, bir sistemin dışarıdan erişilebilen ve saldırıya uğrayabilecek noktalarının toplamıdır. Ağ güvenliğinin ilk ilkesi, bu yüzeyi küçültmektir.

Güvenlik duvarı

Güvenlik duvarı (firewall), ağlar arasından geçen trafiği belirlenmiş kurallara göre izin veren ya da engelleyen sistemdir. Bir binanın girişindeki güvenlik görevlisine benzer: kimin hangi kapıdan, hangi amaçla girebileceğini bir listeye göre kontrol eder.

İyi bir güvenlik duvarı yapılandırmasının temel ilkeleri:

- **Varsayılan olarak reddet:** Açıkça izin verilmeyen her trafik engellenir. Gerekli olanlar tek tek açılır. Tersine, yani "her şey açık, bilinen kötüler kapat" yaklaşımı, unutulmuş bir kapıyı açık bırakır.
- **İçeriden dışarıya da kontrol:** Yalnız dışarıdan gelen trafik değil, içeriden dışarı giden trafik de denetlenir. Ele geçirilmiş bir bilgisayarın saldırganın sunucusuyla konuşmasını engellemek bu sayede mümkün olur.
- **Her kuralın sahibi ve gerekçesi:** "Bu port neden açık, kim istedi, ne zamana kadar?" sorusunun cevabı kayıtlı olmalıdır. Yıllar içinde biriken ve kimsenin hatırlamadığı kurallar güvenlik açığıdır.
- **Yönetim arayüzü internete kapalı:** Güvenlik duvarının, modem ya da sunucuların yönetim ekranları internetten doğrudan erişilebilir olmamalıdır.

Güvenlik duvarları zamanla gelişti. İlk nesil cihazlar yalnız adres ve porta bakardı. Bugün yaygın olan **yeni nesil güvenlik duvarları** (Next-Generation Firewall, NGFW) hangi uygulamanın konuştuğunu tanıyabilir, kullanıcı kimliğine göre kural uygulayabilir ve bilinen saldırı örüntülerini engelleyebilir. Web uygulamalarını korumak için ayrıca **web uygulaması güvenlik duvarı** (Web Application Firewall, WAF) kullanılır; bu sistem web sitesine gelen istekleri inceler ve bilinen saldırı kalıplarını süzer.

Her bilgisayarın üzerinde de bir güvenlik duvarı bulunur. İşletim sistemlerinin kendi güvenlik duvarları açık tutulmalıdır; özellikle dizüstü bilgisayarlar ofis dışındaki ağlara bağlandığında bu önemlidir.

Ağ segmentasyonu

Pek çok küçük kurumda bütün cihazlar tek ve düz bir ağdadır: muhasebe bilgisayarı, misafir telefonu, güvenlik kamerası, yazıcı ve sunucu birbirini görebilir. Bu durumda tek bir cihazın ele geçirilmesi, saldırganı bütün ağı açar.

Segmentasyon, ağı birbirinden ayrılmış bölümlere bölmek ve bölümler arası trafiği kurallarla sınırlamaktır. Gemilerin gövdesindeki su geçirmez bölmeler gibi çalışır: bir bölmeye su dolsa da gemi batmaz.

Tipik bir kurumsal segmentasyon şöyle olabilir:

- **Çalışan ağı:** Ofis bilgisayarları.
- **Sunucu ağı:** Dosya sunucusu, muhasebe veritabanı. Çalışanlar yalnız ihtiyaç duydukları hizmetlere, belirli portlardan erişir.
- **Misafir ağı:** Ziyaretçilerin internet erişimi. Kurumun iç ağıyla hiçbir bağlantısı yoktur.
- **Nesnelerin interneti (IoT) ağı:** Kameralar, akıllı ekranlar, kartlı geçiş sistemleri, klimalar. Bu cihazların güvenliği çoğunlukla zayıftır ve güncellenmeleri ihmal edilir; ayrı tutulmaları gerekir.
- **Yönetim ağı:** Ağ cihazlarının ve sunucuların yönetim arayüzleri. Yalnız yetkili yöneticiler erişir.
- **Üretim ağı:** Fabrikalarda makineleri ve üretim hattını kontrol eden sistemler. Bu ortamlara operasyonel teknoloji (Operational Technology, OT) denir; ofis ağından sıkı biçimde ayrılmalı gerektir, çünkü bir aksaklık doğrudan üretimi durdurur.

Segmentasyon genellikle sanal yerel ağlar (VLAN) ve bu ağlar arasına konan güvenlik duvarı kurallarıyla yapılır. Fidyeye yazılım saldırılarında segmentasyonun etkisi çok açıktır: düz bir ağda bütün sistemler şifrelenirken, iyi bölünmüş bir ağda zarar bir bölümde kalabilir.

VPN

Sanal özel ağ (Virtual Private Network, VPN), internet üzerinden iki nokta arasında şifreli bir tünel kurar. İki yaygın kullanımı vardır:

- **Uzaktan erişim VPN'i:** Evden ya da sahadan çalışan kişinin kurum ağına güvenli bağlanması.
- **Siteler arası VPN:** Bir firmanın İstanbul merkezi ile Kocaeli deposu gibi iki ofisinin ağlarını güvenli biçimde birbirine bağlaması.

VPN hakkında iki önemli nokta var. Birincisi, VPN trafiği şifreler ama bağlanan kişinin kim olduğunu ve cihazının temiz olup olmadığını kendi başına garanti etmez. Ele geçirilmiş bir parolayla bağlanan saldırgan da şifreli tünelden içeri girer. Bu yüzden VPN girişinde MFA zorunlu olmalıdır. İkincisi, VPN cihazları internete açık durduğu için saldırganların sürekli taradığı hedeflerdir. Bu cihazlardaki güvenlik güncellemeleri yayımlandığında beklemeden uygulanmalıdır.

Kişisel kullanım için pazarlanan VPN hizmetleri kurumsal VPN ile aynı şey değildir; onaylanmamış bir VPN uygulaması, iş trafiğini tanımadığın bir şirket üzerinden geçirir.

Kablosuz ağ güvenliği

Kablosuz ağ (Wi-Fi), sinyalin binanın dışına da taşabilmesi nedeniyle özel dikkat ister.

- **Güncel şifreleme:** Kablosuz ağ en az WPA2, mümkünse WPA3 ile korunur. Eski ve kırılmış olan WEP kullanılmaz.
- **Güçlü ve gizli ağ parolası:** Kafe tabelasına yazılır gibi duvara asılan ağ parolası, ofis ağı için kabul edilemez.
- **WPS kapalı:** Düğmeyle ya da kısa PIN ile bağlanmayı sağlayan WPS özelliği bilinen zayıflıklar taşır; kapatılması önerilir.
- **Varsayılan yönetici parolası değiştirilir.** Modem ve erişim noktalarının fabrikadan gelen yönetici parolası ilk kurulumda değiştirilir.
- **Misafir ağı ayrı:** Ziyaretçilere ve çalışanların kişisel telefonlarına ayrı bir misafir ağı verilir.
- **Büyük kurumlarda kişiye özel kimlik:** Herkesin aynı ağ parolasını kullanması yerine, her çalışan kendi kurumsal kimliğiyle kablosuz ağa bağlanır. Bu yöntemde işten ayrılan kişinin erişimi tek hamlede kapanır.

Halka açık kablosuz ağlar (otel, havalimanı, kafe) için kurallar ayrıdır. Bu ağlarda aynı isimde sahte bir erişim noktası kurulmuş olabilir ve trafiğin bir kısmı izlenebilir. İş cihazıyla böyle bir ağa bağlanman gerekiyorsa kurumsal VPN'i aç; mümkünse telefonunun mobil veri paylaşımını tercih et. Kurumsal sistemlere, özellikle bankacılık ve muhasebe ekranlarına, VPN olmadan halka açık ağdan girme.

Saldırı tespit ve önleme

Saldırı tespit sistemi (Intrusion Detection System, IDS), ağ trafiğini izler ve şüpheli örüntü gördüğünde alarm üretir. **Saldırı önleme sistemi** (Intrusion Prevention System, IPS) ise bu trafiği aynı anda engelleyebilir. Bugün bu işlevler çoğunlukla yeni nesil güvenlik duvarlarının içinde yer alır. Ürettikleri alarmlar, Modül 7'de anlatılacak izleme sürecine akar.

Sıfır güven yaklaşımı

Geleneksel ağ güvenliği "kale ve hendek" mantığıyla çalışırdı: dışarı tehlikeli, içerisi güvenli. Bulut hizmetleri, uzaktan çalışma ve mobil cihazlar bu sınırı belirsizleştirdi. **Sıfır güven** (zero trust) yaklaşımı, bir kullanıcının ya da cihazın ağın içinde olmasını tek başına güven sebebi saymaz. Her erişim isteğinde kimlik, cihazın durumu ve isteğin bağlamı yeniden doğrulanır; erişim yalnız gereken kaynakla sınırlı tutulur.

Sıfır güven bir ürün değil, bir tasarım anlayışıdır. Bu eğitimde gördüğün MFA, en az yetki ve segmentasyon, sıfır güvenin temel taşlarıdır.

Uygulama: KOBİ ofis ağını yeniden düzenlemek

Kayseri'de 25 kişilik bir mobilya üreticisinin ofisinde ve atölyesinde bütün cihazlar tek bir ağdadır. Misafirler de aynı kablosuz ağa bağlanır, parolası toplantı odasının duvarında yazılıdır. Atölyedeki CNC tezgâhlarının bilgisayarları da aynı ağdadır. Dış destek firmasıyla şu plan yapılır:

1. Ağdaki bütün cihazların listesi çıkarılır. Listede kimsenin hatırlamadığı iki eski kamera kaydedici ve kullanılmayan bir sunucu bulunur.
2. Ağ beş bölüme ayrılır: ofis bilgisayarları, sunucular, atölye makineleri, kameralar ve misafir ağı.

3. Atölye makineleri yalnız tasarım dosyalarının tutulduğu sunucuya, belirli bir porttan erişebilir; internete doğrudan çıkışı kapatılır.
4. Kameralar internete yalnız üreticinin güncelleme sunucusu için çıkabilir.
5. Misafir ağının yeni parolası düzenli değiştirilir ve iç ağa hiçbir erişimi olmaz.
6. Modemdeki internete açık uzak masaüstü bağlantısı kapatılır; uzaktan çalışanlar MFA'lı VPN ile bağlanır.
7. Kullanılmayan sunucu kapatılır, eski kayıt cihazları güncellenir ya da değiştirilir.

Bu düzenlemenin çoğu, mevcut cihazların doğru yapılandırılmasıyla yapılır.

Sık yapılan hatalar

- **Uzak masaüstü gibi yönetim hizmetlerini doğrudan internete açmak.** Bu hizmetler saldırganların en çok taradığı kapılardır; VPN ve MFA arkasında olmalıdır.
- **Güvenlik duvarında "geçici" açılan kuralları kapatmamak.** Geçici kurallar yıllarca kalır.
- **Misafirleri iç ağa almak.** Ziyaretçinin dizüstü bilgisayarındaki bir zararlı yazılım doğrudan sunucuya ulaşabilir.
- **Kameraları ve akıllı cihazları unutmak.** Varsayılan parolayla internete açık bir kamera, ağa giriş kapısı olabilir.
- **VPN'i güvenliğin kendisi sanmak.** VPN şifreli bir yoldur; yolun ucundaki kişiyi ve cihazı ayrıca doğrulamak gerekir.
- **Halka açık kablosuz ağda kurumsal sistemlere VPN'siz girmek.**

Kendini dene

1. Güvenlik duvarında "varsayılan olarak reddet" ilkesi ne demektir?
2. Ağ segmentasyonunun fidye yazılımı saldırısında sağladığı temel fayda nedir?
3. VPN girişinde neden MFA kullanılmalıdır?
4. Kablosuz ağlar için önerilen şifreleme standartları hangileridir?
5. Sıfır güven yaklaşımı, ağın içindeki bir cihaza nasıl bakar?

Uç nokta ve e-posta güvenliği, güncelleme yönetimi

Uç nokta (endpoint), kullanıcının doğrudan çalıştığı cihazdır: masaüstü ve dizüstü bilgisayarlar, telefonlar, tabletler, hatta depo çalışanının el terminali. Saldırıların çoğu bir uç noktada başlar, çünkü e-posta orada açılır, dosya orada indirilir, parola orada yazılır. Bu modülde uç noktaları, en büyük giriş kapısı olan e-postayı ve bütün bunların temelinde duran güncelleme düzenini ele alacağız.

Bir bilgisayarda olması gereken temel korumalar

Kurumsal bir bilgisayar için şu korumalar temel kabul edilir:

- **Zararlı yazılım koruması:** Klasik antivirüs bilinen zararlı dosyaları imzalarıyla tanır. Bugün kurumlarda daha yaygın olan **uç nokta tespit ve müdahale** (Endpoint Detection and Response, EDR) araçları ise davranışa bakar: bir ofis belgesinin gizlice komut satırı açması ya da bir programın kısa sürede yüzlerce dosyayı şifrelemeye başlaması gibi şüpheli hareketleri fark eder, kaydeder ve gerekirse cihazı ağdan ayırır.
- **Disk şifreleme:** Dizüstü bilgisayar çalınırsa ya da kaybolursa diskteki veriler okunamaz. İşletim sistemlerinin kendi disk şifreleme özellikleri bu iş için yeterlidir; önemli olan açık olduğunu ve kurtarma anahtarının güvenli bir yerde tutulduğunu doğrulamaktır.
- **Ekran kilidi:** Kısa bir hareketsizlikten sonra ekran kendiliğinden kilitlenir. Masadan kalkarken kilitlemek alışkanlık olmalıdır.
- **Yerel yönetici yetkisi olmaması:** Kullanıcı kendi başına program kuramaz. Bu tek ayar, pek çok zararlı yazılımın çalışmasını ya da kalıcı hâle gelmesini zorlaştırır.
- **Güvenlik duvarı açık:** Modül 4'te anlatıldığı gibi cihazın kendi güvenlik duvarı devrede olur.
- **Güncel işletim sistemi ve uygulamalar:** Bu modülün son bölümünde ayrıntılı anlatılıyor.
- **Uygulama denetimi:** Daha olgun ortamlarda yalnız onaylı uygulamaların çalışmasına izin verilir. Buna izin listesi (allowlist) yaklaşımı denir.

Kurumlar bu ayarları merkezi yönetim araçlarıyla bütün cihazlara uygular; uymayan cihazlar raporda görünür.

Mobil cihazlar

İş e-postası, ekip sohbeti ve onay uygulamaları artık telefonda. Bu yüzden telefonlar da birer uç noktadır.

- Ekran kilidi ve cihaz şifrelemesi açık olur.
- Uygulamalar yalnız resmî uygulama mağazasından yüklenir.
- İşletim sistemi güncellemeleri ertelenmez. Üreticinin güncelleme desteğini bitirdiği eski telefonlar iş için kullanılmamalıdır.
- Kurumlar **mobil cihaz yönetimi** (Mobile Device Management, MDM) araçlarıyla bu kuralları uygular, kaybolan telefondaki kurumsal verileri uzaktan silebilir.

Çalışanın kendi telefonunu iş için kullanmasına **kendi cihazını getir** (Bring Your Own Device, BYOD) denir. Bu durumda kurumun, kişisel veriye dokunmadan yalnız kurumsal uygulamaları ve verileri yönetebileceği bir yöntem seçmesi gerekir. Kuralların çalışana yazılı olarak bildirilmesi, hem

güvenlik hem kişisel verilerin korunması açısından önemlidir.

Çıkarılabilir medya ve fiziksel güvenlik

USB bellek ve harici diskler, veri sızıntısının ve zararlı yazılım bulaşmasının kolay yollarıdır. Pek çok kurum USB depolamayı tamamen kapatır ya da yalnız şifreli ve kayıtlı belleklere izin verir. Masada açık bırakılan belgeler, yazıcıda unutulmuş bordro çıktısı ve kilitlenmemiş ekran da uç nokta güvenliğinin fiziksel yüzüdür. **Temiz masa, kilitli ekran** kuralı bu riskleri basitçe azaltır.

E-posta güvenliği

E-posta, saldırıların en yaygın giriş kapısıdır. Korumalar iki katmanda çalışır: teknik filtreler ve kullanıcının dikkati.

Teknik tarafta:

- **E-posta güvenlik filtresi:** Gelen postalardaki zararlı ekleri, bilinen kötü bağlantıları ve spamı ayıklar. Şüpheli ekleri kullanıcıya ulaşmadan önce yalıtılmış bir ortamda açıp davranışına bakan sistemler de vardır.
- **Riskli ek türlerinin engellenmesi:** Çalıştırılabilir dosyalar ve iş için gerekmeyen sıkıştırılmış dosya türleri e-posta ekinde kabul edilmez.
- **Makroların kapatılması:** Ofis belgelerindeki makrolar uzun süre zararlı yazılımın en sevdiği taşıyıcı oldu. İnternette gelen belgelerde makrolar varsayılan olarak kapalı tutulur; "içeriği etkinleştir" uyarısını gördüğünde dur ve sor.
- **Dış e-posta uyarısı:** Kurum dışından gelen postalara "Bu e-posta kurum dışından geldi" etiketi eklenir. Genel müdürün adıyla gelen ama bu etiketi taşıyan bir mesaj, hemen dikkat çeker.

Alan adı sahteciliğine karşı üç kayıt birlikte kullanılır. Bunlar alan adının DNS ayarlarına eklenen kayıtlardır:

- **SPF (Sender Policy Framework):** Alan adı adına hangi sunucuların e-posta gönderebileceğini ilan eder.
- **DKIM (DomainKeys Identified Mail):** Giden e-postaya bir dijital imza ekler; alıcı, mesajın yolda değiştirilmediğini ve gerçekten o alan adından geldiğini doğrulayabilir.
- **DMARC (Domain-based Message Authentication, Reporting and Conformance):** SPF ve DKIM kontrolünü geçemeyen postalara alıcı sunucunun ne yapacağını söyler (izle, karantinaya al, reddet) ve alan adı sahibine rapor gönderir.

Bu üç kayıt, saldırganın senin alan adını birebir taklit etmesini zorlaştırır. Ancak "fırna.com" gibi benzer görünen bir alan adı kaydedilmesini engellemez; orada yine kullanıcının dikkati devreye girer.

Kullanıcı tarafında:

- Şüpheli e-postayı silmek yerine kurumun belirlediği yolla (çoğu e-posta programındaki "bildir" düğmesi ya da bilgi işleme yönlendirme) bildir. Bildirim, aynı e-postanın başka kimlere geldiğini bulmayı sağlar.
- Bağlantıya tıklamadan önce üzerine gelip gerçek adrese bak. Emin değilsen, ilgili siteye bağlantı yerine kendin adres yazarak ya da kayıtlı uygulamadan gir.
- Kişisel veri ya da gizli bilgi içeren dosyaları gönderirken alıcı adresini iki kez kontrol et. Otomatik tamamlama, yanlış kişiye gönderimin en yaygın sebebidir.

Güncelleme (yama) yönetimi

Yazılımlarda zaman zaman güvenlik açıkları bulunur. Üretici bu açığı kapatan bir güncelleme, yani **yama** (patch) yayımlar. Yama yayımlandığı anda açık da herkesin bildiği bir şey hâline gelir ve saldırganlar güncellenmemiş sistemleri aramaya başlar. Güncellemeyi geciktirmek, kapısının kilidinin bozuk olduğu ilan edilmiş bir evde oturmaya benzer.

Bilinen güvenlik açıklarına, kamuya açık bir katalogda **CVE** (Common Vulnerabilities and Exposures) numarası verilir. Böylece farklı ürünler ve ekipler aynı açıktan bahsederken karışıklık olmaz. Üreticinin henüz yamasının bulunmadığı ve saldırganların zaten kullandığı açıklara **sıfırıncı gün** (zero-day) açığı denir. Bu durumda üreticinin önerdiği geçici önlemler uygulanır ve yama çıkar çıkmaz yüklenir.

Düzenli bir yama yönetimi şu adımlardan oluşur:

1. **Envanter:** Hangi cihazda hangi işletim sistemi ve hangi yazılım var? Bilmediğin bir sistemi güncelleyemezsin.
2. **Takip:** Üreticilerin güvenlik duyurularını izle. Büyük işletim sistemi ve ofis yazılımı üreticileri genellikle düzenli takvimlerle güncelleme yayımlar.
3. **Önceliklendirme:** Her yama aynı aciliyette değildir. İnternete açık sistemler (VPN cihazı, e-posta sunucusu, web sitesi), aktif olarak istismar edildiği bilinen açıklar ve kritik dereceli açıklar önce gelir.
4. **Test:** Kritik iş sistemleri için yama önce küçük bir grup cihazda denenir. Test, erteleme bahanesi olmamalıdır; kısa ve planlı tutulur.
5. **Dağıtım:** Merkezi yönetim aracıyla bütün cihazlara uygulanır. Yeniden başlatma gerektiren güncellemeler için kullanıcıya makul bir süre verilir, sonra zorunlu hâle gelir.
6. **Doğrulama:** Hangi cihazların güncellendiği raporlanır. Güncellenemeyenler ayrıca ele alınır.

Üreticinin artık güvenlik güncellemesi yayımlamadığı, yani **desteği biten** yazılımlar ayrı bir risktir. Yeni bulunan açıkları kapanmaz. Bu sistemler ya yenilenir ya da yenilenene kadar ağıdan yalıtılır ve riski yazılı olarak kabul edilir.

Yalnız işletim sistemi değil; tarayıcılar, ofis programları, PDF okuyucular, ağ cihazlarının yazılımları, yazıcılar ve kameralar da güncelleme gerektirir. Web sitelerinde kullanılan içerik yönetim sistemleri ve eklentileri de bu listeye girer.

Uygulama: aylık güncelleme döngüsü

Gaziantep'te 60 kişilik bir tekstil firmasının iki kişilik bilgi işlem ekibi şu döngüyü kurar:

1. Her ayın ilk haftası, üreticilerin yayımladığı güvenlik güncellemeleri listelenir.
2. Aktif istismar edildiği duyurulan ya da internete açık sistemleri etkileyen açıklar "acil" olarak işaretlenir ve 48 saat içinde uygulanır.
3. Diğer güncellemeler önce bilgi işlem ekibinin ve gönüllü beş kişinin bilgisayarlarında üç gün denenir.
4. Sorun çıkmazsa bütün bilgisayarlara dağıtılır; kullanıcılar iki gün içinde yeniden başlatmazsa sistem mesai sonrasında yeniden başlatır.
5. Ay sonunda, güncellenmemiş cihaz listesi çıkarılır ve tek tek takip edilir.
6. Desteği biten iki eski bilgisayar, yenileri gelene kadar internete erişimi kapalı bir bölümde tutulur.

Böylece kimin neyi ne zaman güncellediği görünür hâle gelir.

Sık yapılan hatalar

- **"Şimdi değil" düğmesine haftalarca basmak.** Ertelenen her güncelleme, bilinen bir açığın açık kalması demektir.
- **Yalnız işletim sistemini güncellemek.** Tarayıcı, ofis programı ve ağ cihazları unutulur.
- **İnternette gelen belgede makroları etkinleştirmek.** Belge seni bunu yapmaya yönlendiriyorsa bu bir uyarı işaretidir.
- **Şüpheli e-postayı bildirmeden silmek.** Aynı mesaj başka bir çalışanın kutusunda tıklanmayı bekliyor olabilir.
- **Disk şifrelemesini açıp kurtarma anahtarını saklamamak.** Cihaz arızasında veri sahibine de kapanır.
- **Destegi biten sistemleri "çalışıyor" diye ağda bırakmak.**

Kendini dene

1. EDR, klasik antivirüsten temel olarak hangi yönüyle ayrılır?
2. Çalınan bir dizüstü bilgisayardaki verileri korumak için hangi önlem kullanılır?
3. SPF, DKIM ve DMARC kayıtları hangi tür saldırıyı zorlaştırmaya yöneliktir?
4. Henüz yaması olmayan ve saldırganların kullandığı açığa ne ad verilir?
5. Yama yönetiminde önceliklendirmede hangi sistemler öne alınır?

Yedekleme ve iş sürekliliği

Her güvenlik önlemi bir gün aşılabılır. Bir fidye yazılımı sunucuları şifreleyebilir, bir disk arızalanabilir, bir çalışan yanlış klasörü silebilir, depoyu su basabilir. Bu durumlarda işi kurtaran şey, sağlam ve denenmiş bir yedektir. Yedekleme, erişilebilirlik ve bütünlük ilkelerinin son savunma hattıdır.

Veriyi neye karşı yedekliyoruz?

Yedeğin işe yaraması için hangi senaryoya karşı alındığını bilmek gerekir. Her senaryo farklı bir yedek özelliği ister.

- **Donanım arızası:** Disk ya da sunucu bozulur. Aynı binadaki ikinci bir diske alınmış yedek bu durumda yeterli olabilir.
- **İnsan hatası:** Bir dosya silinir ya da üzerine yanlış veri yazılır, durum günler sonra fark edilir. Geçmişe dönük birden fazla sürüm gerekir.
- **Fidye yazılımı:** Saldırgan ağdaki her şeyi şifreler, ulaşabildiği yedekleri de siler ya da şifreler. Saldırganın erişemeyeceği bir yedek gerekir.
- **Yangın, sel, deprem, hırsızlık:** Binadaki her şey kaybolur. Başka bir konumda bir kopya gerekir.

Deprem riski yüksek Türkiye'de son madde her kurum için gerçekçidir; sunucunun yanındaki harici diskte duran yedek de bu senaryoda kaybolur.

Yedek türleri

- **Tam yedek:** Seçilen verinin tamamının kopyası. Geri yüklemesi en kolay olandır ama en çok yer ve zaman alır.
- **Artımlı yedek:** Yalnız son yedekten (tam ya da artımlı) bu yana değişen veriler. Hızlıdır ve az yer kaplar; geri yüklemek için son tam yedek ve arkasından gelen bütün artımlı yedekler gerekir.
- **Fark yedeği:** Son tam yedekten bu yana değişen bütün veriler. Artımlıdan daha çok yer kaplar ama geri yükleme için yalnız son tam yedek ve son fark yedeği yeterlidir.

Yaygın bir düzen, haftada bir tam yedek ve her gece artımlı yedek almaktır. Hangi düzenin seçileceği, verinin ne kadar sık değiştiğine ve ne kadar hızlı geri dönülmesi gerektiğine bağlıdır.

Bir de **sürüm saklama** konusu var: kaç günlük, kaç haftalık, kaç aylık yedek tutulacak? Fidye yazılımı ve insan hatası durumunda sorun ancak günler ya da haftalar sonra fark edilebilir. Yalnız çünkü yedeği tutan bir düzen, dün zaten bozulmuş olan veriyi yedeklemiş olabilir.

3-2-1 kuralı

Yedekleme için en bilinen ve en kullanışlı kural **3-2-1 kuralıdır**:

- **3** kopya veri: asıl veri ve iki yedek.
- **2** farklı ortam: örneğin bir yedek ağdaki depolama cihazında, bir yedek bulutta ya da teypte.
- **1** kopya başka bir konumda: binanın dışında.

Fidye yazılımlarının yedekleri hedef alması yüzünden bu kural sıklıkla genişletilir. Yaygın genişletilmiş biçimi **3-2-1-1-0** olarak anılır:

- Bir kopya **çevrimdışı ya da değiştirilemez** olur. Çevrimdışı yedek, ağa bağlı olmayan bir ortamdır (bağlantısı kesilen disk, kasadaki teyp). Değiştirilemez (immutable) yedek ise belirlenen süre dolmadan yönetici yetkisiyle bile silinemez ya da değiştirilemez. Saldırgan ağı ele geçirse de bu kopyaya dokunamaz.
- Geri yükleme testlerinde **sıfır hata** hedeflenir: yedeğin gerçekten geri yüklenebildiği düzenli olarak doğrulanır.

Yedek sistemine erişim de korunmalıdır. Yedek yazılımının yönetim hesabı, normal etki alanı hesaplarından ayrı tutulur ve MFA ile korunur. Aksi hâlde yönetici hesabını ele geçiren saldırgan, şifrelemeye başlamadan önce yedekleri sessizce siler.

Yedekler de şifrelenmelidir. Bina dışına götürülen bir yedek diskin ya da bulut hesabının içinde bütün müşteri verisi bulunur; kaybolması bir veri ihlalidir.

RPO ve RTO

Bir kurtarma planı iki soruya cevap vermelidir.

- **RPO (Recovery Point Objective, kurtarma noktası hedefi):** En fazla ne kadar süreli veri kaybını kabul edebiliriz? RPO 24 saat ise, gece alınan yedek yeterlidir; gün içinde girilen veriler kaybolabilir. RPO 1 saat ise, saatlik yedek ya da sürekli kopyalama gerekir.
- **RTO (Recovery Time Objective, kurtarma süresi hedefi):** Sistem en geç ne kadar sürede yeniden çalışmalıdır? Bir e-ticaret sitesi için birkaç saat, bir arşiv sistemi için birkaç gün kabul edilebilir.

RPO yedeğin ne sıklıkla alınacağını, RTO ise yedeğin nerede tutulacağını ve geri yükleme yönteminin ne kadar hızlı olması gerektiğini belirler. Çok kısa RPO ve RTO pahalıdır; bu yüzden her sistem için ayrı belirlenir. Bu değerler bilgi işlemin değil, işin sahibinin vereceği kararlardır: "Sipariş sistemi kaç saat kapalı kalırsa ne kaybederiz?" sorusunun cevabını satış müdürü verir.

Geri yükleme testi

Hiç denenmemiş bir yedek, var olduğu varsayılan bir yedektir. Gerçek bir olayda şunlar sık yaşanır: yedek işinin aylardır hata verdiği ama kimsenin raporlara bakmadığı anlaşılır, önemli bir klasörün yedek kapsamına hiç eklenmediği ortaya çıkar, geri yüklemenin tahmin edilenden kat kat uzun sürdüğü görülür, şifreli yedeğin anahtarının nerede olduğunu kimse bilmez.

Bu yüzden:

1. Yedek işlerinin başarılı ya da başarısız olduğu her gün kontrol edilir; başarısız iş için alarm üretilir.
2. Belirli aralıklarla rastgele seçilen dosyalar geri yüklenip açılır.
3. Yılda en az bir kez, kritik bir sistem baştan sona, ayrı bir ortamda geri yüklenir ve geçen süre ölçülür. Ölçülen süre RTO ile karşılaştırılır.
4. Test sonuçları tarihli olarak kayda geçirilir.

Senkronizasyon yedek değildir

Bulut depolama hizmetlerinin klasör eşitleme özelliği çok kullanışlıdır ama tek başına yedek sayılmaz. Bilgisayarındaki bir dosya silinir ya da fidye yazılımıyla şifrelenirse, eşitleme bu değişikliği bulut kopyasına da taşır. Bazı hizmetler önceki sürümleri ve silinen dosyaları bir süre tutar; bu yararlı bir güvenlik ağıdır ama süresi ve kapsamı sınırlıdır. Kurumsal veriler için ayrı ve bağımsız bir yedekleme düzeni gerekir.

Aynı şekilde, bulut hizmetlerinde (e-posta, ofis paketleri, müşteri yönetim sistemleri) verinin güvenliği konusunda sorumluluk sağlayıcı ile müşteri arasında paylaşılır. Sağlayıcı altyapının ayakta kalmasından sorumludur; yanlışlıkla silinen ya da ele geçirilmiş bir hesap tarafından bozulan veriler ise çoğu zaman müşterinin sorumluluğundadır. Hizmet sözleşmesinde bu ayrımın nasıl yapıldığını bilmek gerekir.

İş sürekliliği ve felaket kurtarma

Yedek veriyi kurtarır; iş sürekliliği ise işin kendisini ayakta tutar.

- **İş sürekliliği planı:** Bir aksaklık sırasında kritik işlerin nasıl süreceğini anlatır. Sistemler kapalıyken siparişler nasıl alınacak, maaşlar nasıl ödenecek, müşterilere nasıl haber verilecek?
- **Felaket kurtarma planı:** Bilgi teknolojileri sistemlerinin hangi sırayla, nerede ve nasıl yeniden ayağa kaldırılacağını anlatır.
- **İş etki analizi:** Bu planların temelidir. Her iş süreci için "Bu süreç durursa bir saat, bir gün, bir hafta sonra ne olur?" sorusu sorulur. Cevaplar hangi sistemlerin önce kurtarılacağını ve RPO, RTO değerlerini belirler.

Planlar kâğıt üzerinde de bulunmalıdır. Fidye yazılımı bütün sistemleri kilitlediğinde, planın kendisi de şifrelenmiş sunucuda duruyorsa işe yaramaz. Kritik telefon numaraları, tedarikçi irtibatları ve kurtarma adımları basılı ya da kurum sistemlerinden bağımsız bir yerde de tutulur.

Örnek vaka: bölge hastanesinde laboratuvar sistemi

Orta büyüklükte bir bölge hastanesinin laboratuvar bilgi sistemi, bir gece yapılan güncelleme sonrasında açılmaz hâle gelir. Hastanede daha önce yapılan iş etki analizinde laboratuvar sistemi için RTO 4 saat, RPO 15 dakika olarak belirlenmiştir.

1. Nöbetçi bilgi işlem personeli olayı fark edince felaket kurtarma planındaki laboratuvar bölümünü açar.
2. Laboratuvar, iş sürekliliği planına göre kâğıt istem ve sonuç formlarına geçer. Acil servis sonuçları telefonla ve imzalı formla iletilir.
3. Sistem, 15 dakikada bir veri kopyalanan ikinci sunucuya devredilir. Son kopyadan sonra girilen birkaç sonuç kâğıt formlardan elle tamamlanır.
4. Sistem 3 saat sonra çalışır hâle gelir; kâğıt formlarla yürütülen işler sisteme işlenir.
5. Bir hafta sonra yapılan değerlendirmede, kâğıt formların bir kısmının eski sürüm olduğu ve bir bölümde formların nerede durduğunu kimsenin bilmediği görülür. Formlar güncellenir ve her bölüme bir kopya konur.

Sistem geri gelene kadar hasta hizmeti durmamıştır; yedekleme ile iş sürekliliği birlikte çalışmıştır.

Sık yapılan hatalar

- **Yedeği sunucunun yanında tutmak.** Fidyeye yazılımı, yangın ya da hırsızlık hem sunucuyu hem yedeği götürür.
- **Yedek işinin başarılı olduğunu varsaymak.** Raporlara bakılmayan yedek aylarca boş dönebilir.
- **Geri yüklemeyi hiç denememek.** Asıl sorular (ne kadar sürer, anahtar nerede, hangi sırayla) ilk kez olay sırasında sorulur.
- **Eşitlenen bulut klasörünü yedek sanmak.**
- **Yalnız dosyaları yedeklemek.** Veritabanları, e-posta, yapılandırma dosyaları ve bulut hizmetlerindeki veriler unutulur.
- **RPO ve RTO'yu bilgi işleme bırakmak.** Ne kadar kayıp kabul edilebilir sorusunu işin sahibi cevaplamalıdır.
- **Kurtarma planını yalnız şifrelenebilecek sistemlerde saklamak.**

Kendini dene

1. 3-2-1 kuralındaki üç sayı neyi ifade eder?
2. Değiştirilemez yedeğin fidye yazılımına karşı sağladığı avantaj nedir?
3. RPO ile RTO arasındaki fark nedir?
4. Bulut depolama hizmetindeki klasör eşitlemesi neden tek başına yedek sayılmaz?
5. İş etki analizinde her süreç için sorulan temel soru nedir?

Güvenlik izleme ve SOC'un işleyişi

Önleyici kontroller ne kadar iyi olursa olsun, bir gün bir saldırı içeri sızabilir. O andan sonra kritik soru şudur: bunu ne kadar çabuk fark edeceğiz? Saldırganın ağda haftalarca fark edilmeden dolaşması ile birkaç saat içinde yakalanması arasındaki fark, küçük bir olay ile işi durduran bir kriz arasındaki farktır. Bu modül, kurumların saldırıyı nasıl fark ettiğini anlatır.

SOC nedir?

Güvenlik operasyon merkezi (Security Operations Center, SOC), kurumun sistemlerini sürekli izleyen, şüpheli olayları inceleyen ve gerektiğinde müdahaleyi başlatan ekiptir. Büyük kurumların kendi SOC'u olabilir. Küçük ve orta ölçekli kurumlar ise bu hizmeti çoğunlukla dışarıdan, yönetilen güvenlik hizmeti sağlayıcılarından alır.

SOC'un temel işleri şunlardır:

- Sistemlerden gelen kayıtları ve alarmları izlemek.
- Alarmları inceleyip gerçek bir tehdit olup olmadığına karar vermek.
- Gerçek olaylarda ilk müdahaleyi yapmak ve olay müdahale sürecini başlatmak.
- Yeni tehditlere karşı tespit kurallarını geliştirmek.
- Yönetime ve ilgili ekiplere düzenli rapor vermek.

Saldırıları çoğunlukla mesai dışında başladığı için pek çok SOC günün her saati çalışır.

Log nedir?

Log (kayıt), bir sistemin yaptığı işlemleri zaman damgasıyla yazdığı satırlardır. Bir kullanıcının oturum açması, bir dosyanın silinmesi, güvenlik duvarının bir bağlantıyı engellemesi, bir programın çalıştırılması birer log satırı üretir.

Güvenlik izlemesi için önemli log kaynakları:

- **Kimlik sistemleri:** Başarılı ve başarısız oturum açmalar, parola değişiklikleri, MFA olayları, yetki değişiklikleri.
- **Güvenlik duvarı ve VPN:** İzin verilen ve engellenen bağlantılar, uzaktan bağlanan kullanıcılar.
- **Uç nokta güvenlik araçları (EDR):** Şüpheli süreçler, engellenen zararlı yazılımlar.
- **E-posta sistemi:** Gelen ve giden postalar, engellenen ekler, oluşturulan yönlendirme kuralları.
- **Sunucular ve uygulamalar:** Yönetici işlemleri, veritabanı erişimleri, web sunucusu istekleri.
- **Bulut hizmetleri:** Yönetim panelindeki değişiklikler, yeni oluşturulan hesaplar ve anahtarlar.

Logların işe yaraması için birkaç şart vardır. Birincisi, bütün sistemlerin saatleri aynı zaman kaynağına göre ayarlanmalıdır; buna **zaman eşitleme** denir ve genellikle NTP (Network Time Protocol) ile yapılır. Saatleri farklı olan sistemlerin logları yan yana konduğunda olayların sırası anlaşılamaz. İkincisi, loglar yeterince uzun süre saklanmalıdır; olaylar çoğu zaman haftalar sonra fark edilir. Üçüncüsü, loglar saldırganın silemeyeceği merkezi bir yerde tutulmalıdır, çünkü saldırganlar izlerini silmeye çalışır. Saklama süresiyle ilgili yasal yükümlülükler sektöre göre değişebilir; bunun için kurumun hukuk birimine danışılır.

SIEM kavramı

Orta büyüklükte bir kurumda bile günde milyonlarca log satırı üretilir. Bunları tek tek okumak imkânsızdır. **SIEM** (Security Information and Event Management, güvenlik bilgisi ve olay yönetimi), farklı kaynaklardan gelen logları tek bir yerde toplayan, anlamlandıran ve şüpheli durumlarda alarm üreten sistemdir.

Bir SIEM'in temel işlevleri:

1. **Toplama:** Bütün kaynaklardan logları merkezi olarak alır.
2. **Normalizasyon:** Her sistemin farklı biçimde yazdığı logları ortak bir biçime çevirir. Örneğin bir sistem "kullanıcı", diğeri "user_name" yazsa da ikisi aynı alana yerleştirilir.
3. **Korelasyon:** Tek başına önemsiz görünen olayları birleştirip anlamlı bir örüntü bulur. "Aynı hesapla 10 dakikada 30 başarısız giriş, ardından bir başarılı giriş, ardından yeni bir e-posta yönlendirme kuralı" tek tek sıradan, birlikte ise ciddi bir alarm konusudur.
4. **Alarm:** Tanımlanmış kurallara uyan durumlarda analiste uyarı gönderir.
5. **Arama ve raporlama:** Geçmişe dönük inceleme yapmayı ve rapor almayı sağlar.

SIEM'e tanımlanan her tespit senaryosuna **kullanım senaryosu** (use case) denir. "Yurt dışından yönetici girişi", "mesai dışında toplu dosya silme", "aynı anda iki farklı ülkeden aynı hesapla oturum açma" birer kullanım senaryosudur. İyi bir SIEM kurulumu, kurumun gerçek risklerine göre seçilmiş ve sürekli ayarlanan senaryolardan oluşur.

SIEM'e yakın iki kavramı da bil:

- **SOAR** (Security Orchestration, Automation and Response): Tekrarlayan inceleme ve müdahale adımlarını otomatikleştiren sistem. Örneğin şüpheli bir e-posta bildirildiğinde ekteki dosyayı ve bağlantıları otomatik olarak kontrol edip sonucu analiste sunar.
- **XDR** (Extended Detection and Response): Uç nokta, e-posta, kimlik ve bulut verilerini tek bir tespit ve müdahale platformunda birleştiren yaklaşım.

Alarm triyajı

Triyaj, hastanelerin acil servisinden gelen bir kavramdır: hangi hasta önce bakılacak? SOC'ta da aynı mantıkla gelen alarmlar incelenir, gerçek olup olmadığına ve aciliyetine karar verilir.

Alarmların önemli bir kısmı **yanlış pozitif** (false positive): sistem şüpheli bir durum görmüş ama durum zararsızdır. Örneğin yurt dışı fuarına giden satış müdürünün oradan oturum açması. Bunun tersi olan **yanlış negatif** (false negative) daha tehlikelidir: gerçek bir saldırı olduğu hâlde alarm üretilmemiştir. Çok fazla yanlış pozitif üreten kurallar analistleri yorar; buna **alarm yorgunluğu** denir ve gerçek alarmların gözden kaçmasına yol açar. Bu yüzden kurallar sürekli ayarlanır.

Bir alarm incelenirken genellikle şu adımlar izlenir:

1. **Alarmı anla:** Hangi kural tetiklendi? Hangi kullanıcı, hangi cihaz, hangi zaman?
2. **Bağlamı topla:** Bu kullanıcı kim, hangi bölümde, normalde nereden ve ne zaman çalışıyor? Cihaz kimin? Benzer alarm daha önce gelmiş mi?
3. **İlgili logları incele:** Alarmdan önce ve sonra aynı kullanıcı ya da cihazla ilgili neler olmuş?
4. **Karar ver:** Yanlış pozitif mi, şüpheli mi, doğrulanmış olay mı?
5. **Önceliklendir:** Etkilenen varlığın önemi ve olayın yayılma ihtimaline göre aciliyet belirle.

6. **Belgele ve aktar:** Ne gördüğünü, neye baktığını ve neden bu karara vardığını yaz. Gerekirse bir üst kademeye ya da olay müdahale ekibine aktar.

Belgeleme çok önemlidir. "Yanlış pozitif" diye kapatılan bir alarmin neden öyle değerlendirildiği yazılı değilse, aynı örüntü sonra gerçek bir saldırının parçası çıktığında geriye dönüp anlamak mümkün olmaz.

SOC'ta roller ve kademeler

Pek çok SOC, işi kademelere ayırır:

- **Birinci kademe (L1):** Gelen alarmları ilk inceleyen analistler. Triyajı yapar, yanlış pozitifleri ayıklar, şüpheli olayları üst kademeye aktarır. Alana giriş için en yaygın pozisyonudur.
- **İkinci kademe (L2):** Aktarılan olayları derinlemesine inceler, kapsamını belirler, müdahale adımlarını başlatır.
- **Üçüncü kademe (L3):** En deneyimli analistler. Karmaşık olayları çözer, zararlı yazılım davranışını inceler, yeni tespit kuralları yazar ve **tehdit avcılığı** (threat hunting) yapar. Tehdit avcılığı, alarm gelmesini beklemeden, "ağımızda fark edilmemiş bir saldırgan var mı?" sorusuyla proaktif arama yapmaktır.

MITRE ATT&CK

SOC ekipleri saldırgan davranışlarını konuşurken çoğunlukla **MITRE ATT&CK** çerçevesini kullanır. Bu, gerçek saldırılarda gözlenen saldırgan taktiklerini (ilk erişim, kalıcılık, yetki yükseltme, yanal hareket, veri sızdırma gibi) ve bu taktiklerin altındaki teknikleri sınıflandıran, herkese açık bir bilgi tabanıdır. Ekipler bu çerçeveye "hangi saldırgan davranışlarını tespit edebiliyoruz, hangilerinde kör noktamız var?" sorusunu sistemli biçimde cevaplar.

Örnek vaka: gece yarısı gelen oturum açma alarmı

Bir belediyenin güvenlik izleme hizmetini veren SOC'ta, gece 02.40'ta "mesai dışında, alışılmadık konumdan başarılı oturum açma" alarmı düşer. Alarm, mali hizmetlerde çalışan bir kullanıcıyla ilgilidir. SIEM'deki ilgili log satırları sadeleştirilmiş hâliyle şöyledir:

```
02:31:05 oturum_basarisiz  kullanıcı=mh.uzman3  kaynak_ip=203.0.113.24  ulke=yurt_disi
02:31:41 oturum_basarisiz  kullanıcı=mh.uzman3  kaynak_ip=203.0.113.24  ulke=yurt_disi
02:38:12 mfa_onaylandi     kullanıcı=mh.uzman3  yontem=bildirim
02:38:13 oturum_basarili   kullanıcı=mh.uzman3  kaynak_ip=203.0.113.24  ulke=yurt_disi
02:39:50 posta_kurali_olustu kullanıcı=mh.uzman3  kural=dis_adrese_yonlendir
```

Birinci kademe analist şu değerlendirmeyi yapar:

1. Kullanıcı normalde yalnız mesai saatlerinde ve belediye ağından çalışıyor; yurt dışı seyahat kaydı yok.
2. Başarısız denemelerin ardından gelen MFA onayı, bir MFA yorgunluğu girişimine ya da kullanıcının uykulu hâlde bildirim onaylamasına işaret ediyor.
3. Girişten bir buçuk dakika sonra, gelen postaları dış bir adrese yönlendiren kural oluşturulmuş. Bu, ele geçirilmiş e-posta hesaplarında çok sık görülen bir adım.
4. Analist olayı "doğrulanmış olay, yüksek öncelik" olarak işaretler ve ikinci kademeye aktarır.

İkinci kademe, anlaşmalı müdahale prosedürüne göre hesabın oturumlarını sonlandırır, hesabı geçici olarak kilitler, yönlendirme kuralını kaldırır ve sabah mesai başında kullanıcıyla ve belediyenin bilgi işlem müdürüyle görüşme planlar. Sonraki adımlar, Modül 8'de anlatılan olay müdahale sürecine göre yürür.

Sık yapılan hatalar

- **Log toplamayı izleme sanmak.** Kimsenin bakmadığı loglar yalnız olaydan sonra işe yarar.
- **Saatleri eşitlememek.** Farklı sistemlerin logları yan yana konduğunda olay sırası çıkarılamaz.
- **Logları kısa süre saklamak.** Olay haftalar sonra fark edildiğinde başlangıcına ait kayıt kalmamış olur.
- **Her şeyi alarm yapmak.** Binlerce önemsiz alarm, gerçek olanın kaçırılmasına yol açar.
- **Yanlış pozitif gereksiz kapatmak.**
- **Alarmı kullanıcıya sormadan "o zaten yurt dışındadır" diye varsaymak.** Bağlam doğrulanır, tahmin edilmez.

Kendini dene

1. SIEM'in korelasyon işlevi ne işe yarar?
2. Bütün sistemlerin saatlerinin eşitlenmesi neden önemlidir?
3. Yanlış pozitif ile yanlış negatif arasındaki fark nedir? Hangisi daha tehlikelidir?
4. Birinci kademe (L1) SOC analistinin temel görevi nedir?
5. Ele geçirilmiş e-posta hesaplarında sık görülen ve log incelemesinde dikkat edilmesi gereken bir adım söyle.

Olay müdahalesi süreci

Bir güvenlik olayı yaşandığında ilk saatlerde verilen kararlar, olayın küçük kalmasını ya da büyümesini belirler. Panik içinde yapılan doğaçlama müdahale çoğu zaman delilleri yok eder, saldırganı uyarır ya da sorunu büyütür. Bu yüzden kurumlar olay müdahalesini önceden tanımlanmış bir süreçle yürütür.

Olay ve güvenlik olayı

Sistemlerde her an sayısız sıradan **olay** (event) yaşanır: bir oturum açma, bir başarısız parola denemesi. **Güvenlik olayı** (incident) ise bilginin gizliliğini, bütünlüğünü ya da erişilebilirliğini bozan veya bozma tehdidi taşıyan, müdahale gerektiren durumdur. Ele geçirilmiş bir hesap, fidye yazılımı bulaşması, yanlış kişiye gönderilen müşteri listesi ve çalınan dizüstü bilgisayar birer güvenlik olayıdır.

Her olayın aynı ağırlıkta olmadığını da bilmek gerekir. Kurumlar olayları genellikle önem derecesine göre (düşük, orta, yüksek, kritik) sınıflandırır ve her derece için kimin haberdar edileceğini, ne kadar sürede müdahale edileceğini önceden belirler.

Altı aşama

Olay müdahalesi için yaygın olarak kullanılan model altı aşamadan oluşur. NIST ve SANS gibi kaynaklar aşamaları biraz farklı gruplara da mantık aynıdır.

1. Hazırlık
2. Tespit ve analiz
3. Sınırlama
4. Temizleme
5. Kurtarma
6. Ders çıkarma

Aşamalar her zaman kesin sırayla ilerlemez. Temizleme sırasında yeni bir ele geçirilmiş sistem bulunursa ekip yeniden tespit ve sınırlamaya döner.

1. Hazırlık

Olay müdahalesinin en önemli kısmı, olay yaşanmadan önce yapılır.

- **Olay müdahale planı:** Kimin neye karar vereceği, hangi olayda kimin aranacağı, adımların neler olduğu yazılıdır ve yönetim tarafından onaylanmıştır.
- **Ekip ve roller:** Olay sorumlusu, teknik müdahale ekibi, iletişim sorumlusu, hukuk ve yönetim temsilcisi bellidir. Küçük kurumlarda bu roller birkaç kişide toplanır, dış destek firmasının rolü sözleşmede tanımlanır.
- **İrtibat listesi:** Yöneticiler, dış destek firması, internet servis sağlayıcısı, sigorta şirketi, hukuk danışmanı ve gerektiğinde başvurulacak resmî kurumların bilgileri, sistemlerden bağımsız bir yerde de tutulur.

- **Araçlar ve erişimler:** Log kayıtları, uç nokta araçları, temiz bir yönetim bilgisayarı, yedeklere erişim hazırır.
- **Senaryo bazlı adımlar:** Fidyeye yazılımı, ele geçirilmiş e-posta hesabı, kayıp cihaz, veri sızıntısı gibi sık senaryolar için kısa adım listeleri hazırlanır.
- **Tatbikat:** Yılda en az bir kez, masa başı tatbikatiyle bir senaryo üzerinden konuşulur: "Pazartesi sabahı sunucuların şifrelendiğini gördük. İlk bir saatte ne yaparız?" Bu tatbikatlar plandaki boşlukları ortaya çıkarır.

2. Tespit ve analiz

Olay; SOC alarmıyla, bir çalışanın bildirimıyla, bir müşterinin şikâyetiyle ya da dışarıdan gelen bir uyarıyla fark edilebilir. Bu aşamada sorulan sorular şunlardır:

- Gerçekten bir güvenlik olayı mı, yoksa bir arıza ya da yanlış alarm mı?
- Hangi sistemler, hesaplar ve veriler etkilenmiş?
- Olay ne zaman başlamış? Saldırgan hâlâ içeride mi?
- Kişisel veri etkilenmiş mi? Bu soru, Modül 10'da anlatılacak bildirim yükümlülükleri açısından erken sorulmalıdır.
- Önem derecesi nedir?

Bu aşamada **delillerin korunması** kritiktir. Loglar, şüpheli e-postalar, etkilenen sistemlerin bellek ve disk görüntüleri, ileride olayın nasıl yaşandığını anlamak ve gerekirse hukuki süreçte kullanmak için gereklidir. Delil toplama işi, deneyimli kişilerce ve belgelenerek yapılır. Kimin hangi delili ne zaman aldığını ve nerede sakladığını gösteren kayda **delil zinciri** (chain of custody) denir.

Analiz sırasında yapılan her işlem, saatiyle birlikte bir **olay günlüğüne** yazılır. Olay büyüdükçe kimin neyi ne zaman yaptığını hatırlamak imkânsızlaşır.

3. Sınırlama

Sınırlamanın amacı, olayın yayılmasını ve zararın büyümesini durdurmaktır. İki düzeyde düşünülür:

- **Kısa vadeli sınırlama:** Hızlı ve geçici önlemler. Etkilenen bilgisayarı ağdan ayırmak, ele geçirilmiş hesabı kilitlemek ve oturumlarını sonlandırmak, saldırganın bağlandığı dış adresleri güvenlik duvarında engellemek.
- **Uzun vadeli sınırlama:** Temizleme yapılana kadar işin sürmesini sağlayan önlemler. Etkilenen bölümü ayrı bir ağ bölümüne almak, kritik sistemler için geçici kurallar koymak.

Sık sorulan bir soru: şüpheli bilgisayar kapatılmalı mı? Genel kural, cihazı **kapatmak yerine ağdan ayırmaktır**: kabloyu çıkarmak, kabloşuz bağlantıyı kesmek ya da EDR aracıyla yalıtım. Kapatmak, bellekteki değerli delilleri yok edebilir. Kurumun planında farklı bir talimat varsa ona uyulur.

Sınırlama kararları işi de etkiler. Bir e-ticaret sitesinin ödeme sistemini kapatmak, ciddi gelir kaybı demektir. Bu kararlar yetkili yöneticilerle birlikte, riskler tartılarak verilir.

4. Temizleme

Temizleme, saldırganın bıraktığı her şeyin ortamdan çıkarılmasıdır.

- Zararlı yazılımlar kaldırılır; ele geçirildiği kesin olan sistemler çoğunlukla temizlemek yerine sıfırdan kurulur.

- Saldırganın açtığı hesaplar, eklediği yönlendirme kuralları, zamanlanmış görevler ve uzaktan erişim araçları bulunup kaldırılır.
- Ele geçirildiğinden şüphelenilen bütün parolalar değiştirilir; özellikle yönetici ve servis hesapları.
- Saldırganın içeri girdiği açık (güncellenmemiş bir cihaz, MFA'sız bir hesap) kapatılır. Giriş noktası kapatılmadan yapılan temizlik, saldırıdan aynı yoldan geri dönmesiyle sonuçlanabilir.

5. Kurtarma

Kurtarma, sistemlerin güvenli biçimde normal çalışmaya döndürülmesidir.

- Sistemler, iş etki analizindeki önceliğe göre sırayla ayağa kaldırılır.
- Veriler, saldırının başlangıcından önceye ait ve temiz olduğu doğrulanmış yedeklerden geri yüklenir. Yedeğin içinde de saldırıdan bıraktığı bir şey olmadığından emin olunur.
- Geri dönen sistemler bir süre sıkı izlenir. Saldırganın geri dönme girişimleri çoğu zaman bu dönemde görülür.
- İş birimleri sistemlerin doğru çalıştığını onaylar.

6. Ders çıkarma

Olay kapandıktan sonra, genellikle birkaç hafta içinde, ilgili herkesle bir değerlendirme toplantısı yapılır. Amaç suçlu bulmak değil, sistemi iyileştirmektir.

- Ne oldu? Zaman çizelgesi nasıl?
- Olay nasıl ve ne kadar sürede fark edildi? Daha erken fark edilebilir miydi?
- Hangi adımlar iyi işledi, hangileri aksadı?
- Plan, irtibat listesi, araçlar yeterli miydi?
- Bir daha olmaması için hangi önlemler alınacak, kim sorumlu, son tarih ne?

Çıktı, takibi yapılan yazılı bir rapordur.

İletişim

Olay sırasında iletişim, teknik müdahale kadar önemlidir.

- Olay hakkında yalnız yetkili kişi konuşur. Çalışanlar müşterilere, basına ya da sosyal medyaya kendi başlarına bilgi vermez.
- Saldırganın e-posta sistemine erişimi olabileceği varsayılarak, olay ekibi kendi aralarında gerekirse kurum dışı ve güvenli bir kanal kullanır.
- Müşterilere, iş ortaklarına ve resmî kurumlara yapılacak bildirimler hukuk biriminin görüşüyle hazırlanır. Kişisel veri ihlallerinde yasal bildirim yükümlülükleri vardır; ayrıntıları Modül 10'da.

Çalışan olarak ne yapmalısın?

Güvenlik ekibinde olmasan da bir olayın ilk tanığı sen olabilirsin.

1. Şüpheli bir durum gördüğünde (tıkladığın bir bağlantı, açılmayan dosyalar, ekranda fidye notu, beklenmedik MFA isteği) hemen kurumun belirlediği kanaldan bildir.

2. Bilgisayarında fidye notu ya da dosyaların toplu şekilde değiştiğini görürsen ağ kablosunu çıkar ve kablolu bağlantıyı kapat; bilgisayarı kapatma. Kurumunun talimatı farklıysa ona uy.
3. Kendi başına "temizlemeye" çalışma: dosya silme, program kaldırma, internetten araç indirme.
4. Ne gördüğünü, ne zaman gördüğünü ve ne yaptığını not et.
5. Olay hakkında yetkililer dışında kimseyle konuşma.

Örnek vaka: lojistik firmasında fidye yazılımı

İzmir'deki 40 kişilik lojistik firmasında bir pazartesi sabahı, sevkiyat bölümündeki çalışanlar dosya sunucusundaki belgelerin açılmadığını ve her klasörde bir fidye notu olduğunu görür.

1. **Tespit:** Bir çalışan durumu bilgi işlem sorumlusuna bildirir. Sorumlu, notu görür ve olay müdahale planını açar; olay "kritik" olarak sınıflandırılır.
2. **İlk sınırlama:** Dosya sunucusu ve şifreleme belirtisi görülen üç bilgisayar ağdan ayrılır. Uzaktan erişim VPN'i geçici olarak kapatılır. Bütün yönetici hesaplarının parolaları değiştirilir.
3. **Yönetim ve dış destek:** Genel müdüre bilgi verilir, sözleşmeli olay müdahale firması ve sigorta şirketi aranır. Hukuk danışmanı sürece dahil edilir.
4. **Analiz:** Müdahale ekibi, saldırganın üç hafta önce MFA'sız bir VPN hesabıyla, işten ayrılmış bir çalışanın kapatılmamış hesabıyla girdiğini bulur. Saldırgan bu süre içinde sunucudaki müşteri sözleşmelerini dışarı kopyalamıştır.
5. **Kişisel veri değerlendirmesi:** Kopyalanan dosyalarda müşteri temsilcilerinin ad ve iletişim bilgileri bulunduğu için hukuk danışmanı ile birlikte veri ihlali bildirimi hazırlığı başlatılır.
6. **Temizleme ve kurtarma:** Etkilenen sistemler sıfırdan kurulur. Firma, Modül 6'da anlatılan çevrimdışı yedek düzenine birkaç ay önce geçtiği için dosyalar, saldırıdan önceki bir günün temiz yedeğinden geri yüklenir. İş üç gün içinde normale döner.
7. **Ders çıkarma:** Değerlendirme toplantısında üç önlem kararlaştırılır: VPN dahil bütün uzaktan erişimlerde MFA, insan kaynaklarıyla bağlantılı hesap kapatma süreci ve dışarıya büyük veri transferleri için izleme kuralı.

Sık yapılan hatalar

- **Plan olmadan olaya yakalanmak.** İlk saatler kimi arayacağını bulmakla geçer.
- **Şüpheli bilgisayarı kapatmak ya da yeniden kurmak.** Delil kaybolur, olayın nasıl yaşandığı anlaşılamaz.
- **Giriş noktasını bulmadan sistemleri geri açmak.** Saldırgan aynı yoldan geri döner.
- **Olay günlüğü tutmamak.** Sonradan zaman çizelgesi çıkarılamaz, bildirimlerde hata yapılır.
- **Olayı saklamak ya da küçümsemek.** Yasal bildirim süreleri kaçırılabilir, güven kaybı büyür.
- **Ders çıkarma toplantısını atlamak.**

Kendini dene

1. Olay müdahalesinin altı aşamasını sırasıyla say.
2. Şüpheli bir bilgisayarı kapatmak yerine ağdan ayırmak neden önerilir?
3. Delil zinciri neyi gösterir?
4. Temizleme aşamasında saldırganın giriş noktasının kapatılması neden şarttır?
5. Ders çıkarma toplantısının amacı nedir?

Etik hackerlık ve sızma testi

Bir kurumun savunmasının gerçekten işe yarayıp yaramadığını anlamamanın en doğrudan yolu, onu kontrollü biçimde sınamaktır. Bu işi yapan uzmanlara etik hacker, yaptıkları işin en bilinen biçimine de sızma testi denir. Bu modül, etik hackerlığın ne olduğunu, yasal çerçevesini ve bir kurumun sızma testi hizmetini nasıl doğru alacağını kavramsal düzeyde anlatır. Teknik uygulama yöntemleri bu eğitimin kapsamında değildir.

Etik hacker kimdir?

Etik hacker, bir kurumun sistemlerindeki güvenlik açıklarını, **kurumun yazılı izniyle ve belirlenen sınırlar içinde** bulmaya çalışan güvenlik uzmanıdır. Amacı zarar vermek değil, açıkları gerçek bir saldırgandan önce bulup kuruma raporlamak ve kapatılmasına yardım etmektir.

Etik hacker ile saldırganı ayıran şey kullanılan bilgi ya da beceri değil, üç unsurdur:

- **İzin:** Sistem sahibinin önceden verilmiş, yazılı ve açık izni.
- **Kapsam:** Hangi sistemlerin, hangi yöntemlerle, hangi zaman aralığında test edileceğinin net sınırları.
- **Amaç ve gizlilik:** Bulguların yalnız sistem sahibine raporlanması, test sırasında erişilen verilerin korunması ve iş bittiğinde silinmesi.

Bu unsurlardan biri eksikse yapılan iş artık etik hackerlık değildir. "Açığı gösterip yardım etmek istedim" niyeti, izinsiz erişimi meşru kılmaz.

Yasal çerçeve

Türkiye'de bilişim sistemlerine izinsiz erişim ve bu sistemlere zarar verme suçtur. Türk Ceza Kanunu'nun "Bilişim Alanında Suçlar" bölümü (243 ve devamı maddeler) bir bilişim sistemine hukuka aykırı olarak girmeyi, orada kalmaya devam etmeyi, sistemin işleyişini engellemeyi ya da bozmayı ve verileri değiştirmeyi, yok etmeyi suç olarak tanımlar. Başka ülkelerde de benzer yasalar vardır.

Bu yüzden:

- Sahibi olmadığın hiçbir sistemi izinsiz test etme; buna "sadece bakmak", "sadece taramak" da dahildir.
- İzin, sistemin gerçek sahibinden ya da onu yetkilendirebilecek kişiden alınır. Bir çalışanın sözlü onayı yeterli değildir. Bulut hizmetlerinde barındırılan sistemler için hizmet sağlayıcısının test kuralları da ayrıca kontrol edilir.
- Öğrenmek istiyorsan, bu amaçla hazırlanmış yasal eğitim ortamlarını ve kendi kurduğun deneme laboratuvarlarını kullan.

Zafiyet taraması, sızma testi ve kırmızı takım

Bu üç kavram sık karıştırılır.

- **Zafiyet taraması:** Otomatik araçlarla sistemlerin bilinen açıklara karşı taranmasıdır. Geniş kapsamlıdır, düzenli (örneğin aylık) yapılır, çok sayıda bulgu listeler. Bulguların bir kısmı yanlış

pozitif olabilir; açığın gerçekten kullanılabilir olup olmadığını doğrulamaz.

- **Sızma testi (penetration test):** Uzman bir kişi ya da ekibin, belirlenen kapsamda açıkları bulup gerçekten kullanılabilir olup olmadığını kontrollü biçimde doğruladığı testtir. "Bu açıkla saldırgan nereye kadar ulaşabilir?" sorusunu cevaplar. Genellikle yılda bir ve büyük değişikliklerden sonra yapılır.
- **Kırmızı takım çalışması:** Belirli bir hedefe (örneğin "müşteri veritabanına ulaşmak") gerçekçi bir saldırgan gibi, uzun sürede ve çoğunlukla savunma ekibine haber vermeden ulaşmaya çalışan kapsamlı tatbikat. Yalnız açıkları değil, kurumun tespit ve müdahale yeteneğini de sınar. Savunma ekibine **mavi takım** denir; iki ekibin birlikte çalışıp birbirinden öğrendiği düzene de **mor takım** denir.

Yeni başlayan bir kurum için sıra şudur: önce düzenli zafiyet taraması, sonra sızma testi, en son kırmızı takım.

Test türleri

Sızma testleri, testi yapanın önceden ne kadar bilgiye sahip olduğuna göre ayrılır:

- **Kara kutu:** Testçiye neredeyse hiç bilgi verilmez; dışarıdaki bir saldırganın bakış açısı taklit edilir.
- **Beyaz kutu:** Testçiye mimari belgeler, kaynak kod, kullanıcı hesapları gibi ayrıntılı bilgi verilir. Daha derinlemesine ve verimli bir inceleme sağlar.
- **Gri kutu:** İkisinin arası. Örneğin testçiye sıradan bir kullanıcı hesabı verilir ve "ele geçirilmiş bir çalışan hesabıyla saldırgan neler yapabilir?" sorusu incelenir.

Hedefe göre de türler vardır: internete açık sistemlerin dış ağ testi, iç ağ testi, web ve mobil uygulama testi, kablosuz ağ testi ve çalışanların ortalama karşı direncini ölçen sosyal mühendislik testi. Sosyal mühendislik testleri, çalışanları cezalandırmak için değil, eğitim ihtiyacını belirlemek için yapılır; sonuçlar kişi bazında teşhir edilmez.

Kapsam ve angajman kuralları

Bir sızma testine başlamadan önce taraflar, **angajman kuralları** (rules of engagement) adı verilen yazılı bir belge üzerinde anlaşır. Bu belgede en az şunlar bulunur:

- Test edilecek sistemler, adresler ve uygulamalar; kapsam dışı olanlar da açıkça yazılır.
- Testin başlangıç ve bitiş tarihleri, izin verilen saatler.
- İzin verilen ve verilmeyen yöntemler. Örneğin hizmeti durdurabilecek testler ve gerçek müşteri verisinin değiştirilmesi çoğunlukla kapsam dışıdır.
- Kritik bir açık bulunduğunda ya da test bir sisteme beklenmedik biçimde zarar verdiğinde aranacak kişiler ve testin nasıl durdurulacağı.
- Test sırasında erişilebilecek verilerin nasıl korunacağı, raporun nasıl iletileceği ve test verilerinin ne zaman silineceği.
- Gizlilik sözleşmesi ve yetkili kişinin imzası.

Kapsamın dışına çıkmak, iyi niyetle bile olsa, yetkisiz erişim anlamına gelebilir. Testçi kapsam dışı bir sisteme erişim imkânı fark ederse, bunu kullanmaz, raporlar.

Bir sızma testi nasıl ilerler?

Yöntemler kuruluşlara göre değişse de genel akış şöyledir:

1. **Planlama ve kapsam:** Hedefler, kapsam ve kurallar belirlenir.
2. **Bilgi toplama:** Kapsamdaki sistemler hakkında bilgi edinilir.
3. **Zafiyet tespiti:** Olası açıklar belirlenir.
4. **Doğrulama:** Açıkların gerçekten kullanılabilir olup olmadığı, kurallar içinde ve zarar vermeden kanıtlanır.
5. **Raporlama:** Bulgular, etkileri ve kapatma önerileri raporlanır.
6. **Yeniden test:** Kurum açıkları kapattıktan sonra düzeltmelerin işe yarayıp yaramadığı kontrol edilir.

Rapor nasıl okunur?

Kurum açısından sızma testinin asıl ürünü rapordur. İyi bir rapor iki bölümden oluşur: yöneticiler için kısa bir yönetici özeti ve teknik ekip için ayrıntılı bulgular. Her bulgu için genellikle şunlar yer alır:

- Açığın tanımı ve etkilenen sistem.
- **Risk derecesi:** Kritik, yüksek, orta, düşük, bilgi. Derecelendirmede çoğunlukla **CVSS** (Common Vulnerability Scoring System) adlı ortak puanlama sistemi kullanılır; açığın kullanılma kolaylığı ve etkisi 0 ile 10 arasında puanlanır.
- Açığın varlığını gösteren kanıt.
- Kapatma önerisi.

Raporu alan kurum, bulguları önceliklendirir, her biri için sorumlu ve son tarih belirler ve yeniden testle kapatıldığını doğrular. Rapor, bir rafta duran belge olarak kalırsa test parası boşa harcanmış olur.

Sorumlu bildirim ve hata ödül programları

Bazen bir kişi, test etmeye çalışmadan, sıradan bir kullanım sırasında bir kurumun sisteminde açık fark eder. Doğru yaklaşım **sorumlu bildirim** (responsible disclosure): açık kullanılmaz, başkalarıyla paylaşılmaz, kurumun belirlediği güvenlik iletişim kanalından bildirilir ve kuruma kapatması için makul süre tanınır.

Bazı kurumlar **hata ödül programları** (bug bounty) yürütür. Bu programlarda kurum, hangi sistemlerinin hangi kurallarla test edilebileceğini açıkça ilan eder ve geçerli bulgu bildirenlere ödül verir. Bu programlar da birer yazılı izindir; yalnız ilan edilen kapsam ve kurallar içinde geçerlidir.

Alana girmek isteyenler için

Etik hackerlık, ağlar, işletim sistemleri, web uygulamaları ve güvenlik kavramları üzerine sağlam bir temel gerektirir. Bu alanda çalışanların çoğu sistem yönetimi, ağ ya da SOC analistliği gibi rollerden gelir. Yasal laboratuvar ortamlarında pratik yapmak, raporlama becerisi geliştirmek ve etik kurallara titizlikle uymak bu mesleğin parçasıdır. Bir sızma testçisinin itibarı, teknik becerisi kadar güvenilirliğine dayanır.

Uygulama: sızma testi hizmeti alırken kontrol listesi

Konya'da online ödeme alan 30 kişilik bir e-ticaret şirketi, ilk kez sızma testi yaptırmaya karar verir. Bilgi işlem müdürü şu listeyi kullanır:

1. Neden test yaptırıyoruz? Müşteri ya da iş ortağı şartı mı, yeni uygulama mı, genel kontrol mü? Kapsamı bu cevap belirler.
2. Kapsamda neler var? Web sitesi, mobil uygulama, yönetim paneli, internete açık sunucular. Ödeme altyapısı ödeme kuruluşuna aitse, onun kuralları ayrıca kontrol edilir.
3. Hizmet veren firmanın referansları, ekibin deneyimi ve örnek (anonimleştirilmiş) raporu incelenir.
4. Angajman kuralları belgesi, gizlilik sözleşmesi ve yetkili imzalar tamamlanır.
5. Test tarihleri, kampanya dönemleri gibi yoğun günlerin dışında seçilir; izleme ekibine ve hosting sağlayıcısına bilgi verilir.
6. Rapor geldiğinde bulgular önceliklendirilir, kritik ve yüksek bulgular için 30 günlük kapatma planı yapılır.
7. Kapatılan açıklar için yeniden test istenir.

Sık yapılan hatalar

- **İzinsiz "deneme" yapmak.** İyi niyet, yasal sorumluluğu ortadan kaldırmaz.
- **Zafiyet taramasını sızma testi sanmak.** Otomatik tarama raporu, uzmanın doğruladığı testin yerini tutmaz.
- **Kapsamı belirsiz bırakmak.** "Her şeye bakın" ifadesi, hem yasal hem operasyonel risk doğurur.
- **Raporu alıp açıkları kapatmamak.** Test yalnız bir fotoğraftır; değeri, düzeltmelerden gelir.
- **Yeniden test yapmamak.** Kapatıldığı sanılan açık açık kalmış olabilir.
- **Sosyal mühendislik testi sonuçlarını çalışanları cezalandırmak için kullanmak.** Bildirim kültürünü zayıflatır.

Kendini dene

1. Etik hacker ile saldırıyı ayıran üç unsur nedir?
2. Zafiyet taraması ile sızma testi arasındaki temel fark nedir?
3. Testçiye sıradan bir kullanıcı hesabı verilerek yapılan test türüne ne ad verilir?
4. Angajman kuralları belgesinde bulunması gereken üç unsur say.
5. Bir sistemde tesadüfen açık fark eden kişi sorumlu bildirim ilkesine göre nasıl davranmalıdır?

Standartlar, mevzuat ve güvenlik kültürü

Önceki modüllerdeki önlemlerin dağınık değil, bir sistem içinde ve ölçülebilir biçimde uygulanmasını standartlar sağlar; bazı önlemler ise yasal zorunluluktur. Bu modül en sık karşılaşılabilecek standartları, Türkiye'deki temel mevzuatı ve güvenlik kültürünü anlatır.

ISO/IEC 27001 nedir?

ISO/IEC 27001, Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) tarafından yayımlanan, **bilgi güvenliği yönetim sistemi** (BGYS) standardıdır. Bir kurumun bilgi güvenliğini nasıl yöneteceğine dair şartları tanımlar. Dünyada en yaygın kullanılan bilgi güvenliği standardıdır ve kurumlar bu standarda göre belgelendirilebilir. Güncel sürümü 2022'de yayımlanmıştır.

Standardın temel mantığı, Modül 1'de gördüğün risk yaklaşımıdır. Kurum, kendi bilgi varlıklarını ve risklerini belirler, bu risklere karşı kontroller seçer, bunları uygular, etkinliğini ölçer ve sürekli iyileştirir. Bu döngü **Planla, Uygula, Kontrol et, Önlem al** (PUKÖ; İngilizcesi Plan-Do-Check-Act) olarak bilinir.

Standardın ana gövdesi, yönetim sisteminin şartlarını anlatır:

- **Kurumun bağlamı ve kapsam:** BGYS hangi birimleri, lokasyonları, süreçleri ve sistemleri kapsıyor?
- **Liderlik:** Üst yönetimin taahhüdü, bilgi güvenliği politikası, rol ve sorumluluklar.
- **Planlama:** Risk değerlendirmesi ve risk işleme planı, bilgi güvenliği hedefleri.
- **Destek:** Kaynaklar, yetkinlik, farkındalık, iletişim, belgelendirilmiş bilgiler.
- **Operasyon:** Planların uygulanması, risk değerlendirmesinin düzenli tekrarlanması.
- **Performans değerlendirme:** İzleme ve ölçme, iç denetim, yönetimin gözden geçirmesi.
- **İyileştirme:** Uygunsuzlukların düzeltilmesi ve sürekli iyileştirme.

Standardın ekinde (Ek A) bir kontrol listesi bulunur. 2022 sürümünde kontroller dört tema altında toplanır: kurumsal, insanlarla ilgili, fiziksel ve teknolojik kontroller. Erişim yönetimi, yedekleme, log kaydı, zararlı yazılım koruması, tedarikçi ilişkileri ve olay yönetimi gibi bu eğitimde gördüğün konuların hepsi bu listede yer alır.

Kurum, risk değerlendirmesine göre hangi kontrolleri uygulayacağını, hangilerini neden uygulamayacağını **Uygulanabilirlik Bildirgesi** (Statement of Applicability) adlı belgede gösterir. Bu belge, BGYS'nin en önemli belgelerinden biridir.

Kontrollerin nasıl uygulanacağına dair ayrıntılı rehberlik **ISO/IEC 27002** standardında yer alır. 27001 "ne yapılmalı" sorusuna, 27002 "nasıl yapılabilir" sorusuna odaklanır. Belgelendirme 27002'ye göre değil, 27001'e göre yapılır.

Belgelendirme süreci

Bir kurum ISO/IEC 27001 belgesi almak istediğinde genellikle şu yolu izler:

1. Kapsamı belirler ve üst yönetim onayını alır.
2. Risk değerlendirmesini yapar, kontrolleri seçer, politika ve prosedürleri yazar.

3. Sistemi bir süre işletir; kayıtlar oluşmaya başlar.
4. Çalışanları eğitir, iç denetim ve yönetimin gözden geçirmesi toplantısını yapar.
5. Akredite bir belgelendirme kuruluşu iki aşamalı denetim yapar: önce belgeler, sonra uygulama incelenir.
6. Belge verildikten sonra her yıl gözetim denetimleri yapılır; belge genellikle üç yıllık döngüyle yenilenir.

Kâğıt üzerinde düzgün ama uygulamada işlemeyen bir sistem, ilk ciddi olayda ortaya çıkar.

Diğer çerçeveler

- **NIST Siber Güvenlik Çerçevesi (CSF):** ABD Ulusal Standartlar ve Teknoloji Enstitüsü'nün yayımladığı, gönüllü kullanılan bir çerçeve. Güvenlik faaliyetlerini tanımla, koru, tespit et, müdahale et ve kurtar işlevleri etrafında toplar; 2024'teki güncellemeyle bunlara yönetim işlevi eklenmiştir. Kurumun mevcut durumunu ve hedefini anlatmak için kullanışlı bir dil sağlar.
- **PCI DSS (Payment Card Industry Data Security Standard):** Kredi kartı verisini işleyen, saklayan ya da ileten kurumlar için kart şirketlerinin belirlediği güvenlik standardı. Bir e-ticaret şirketi, kart verisini kendi sistemine hiç almayıp ödemeyi bir ödeme kuruluşuna bırakarak bu yükümlülüklerin önemli bir kısmından kaçınabilir; Modül 1'deki "riskten kaçınma" seçeneğinin bir örneğidir.

KVKK ve kişisel verilerin güvenliği

Türkiye'de kişisel veriler **6698 sayılı Kişisel Verilerin Korunması Kanunu** (KVKK) ile korunur. Kanunun uygulanmasını Kişisel Verileri Koruma Kurumu ve onun karar organı olan Kişisel Verileri Koruma Kurulu denetler.

Temel kavramlar:

- **Kişisel veri:** Kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Ad, telefon, e-posta, adres, TC kimlik numarası, IP adresi, kamera görüntüsü.
- **Özel nitelikli kişisel veri:** Sağlık, biyometrik ve genetik veriler, din, siyasi düşünce, ceza mahkûmiyeti gibi kanunda sayılan veriler. Bu veriler için daha sıkı koruma gerekir.
- **Veri sorumlusu:** Verinin neden ve nasıl işleneceğine karar veren gerçek ya da tüzel kişi. Çalışanlarının ve müşterilerinin verisini işleyen şirket, bu verilerin veri sorumlusudur.
- **Veri işleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına veri işleyen kişi ya da kurum. Bordro hizmeti veren dış firma ya da bulut hizmeti sağlayıcısı buna örnek olabilir.

KVKK'nın 12. maddesi, veri sorumlusuna kişisel verilerin hukuka aykırı işlenmesini ve bunlara hukuka aykırı erişilmesini önlemek, verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik **gerekli her türlü teknik ve idari tedbiri** alma yükümlülüğü getirir. Veri işleyen kullanılıyorsa, veri sorumlusu bu tedbirlerin alınmasından onunla birlikte sorumludur. Kurul'un yayımladığı kişisel veri güvenliği rehberi, bu tedbirlerin neler olabileceğini somut olarak anlatır; bu eğitimde gördüğün erişim yönetimi, şifreleme, log kaydı, yedekleme ve farkındalık eğitimi bunların başında gelir.

Veri ihlali bildirimi

KVKK'nın 12. maddesine göre, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusu bu durumu **en kısa sürede ilgili kişiye ve Kurula bildirir**. Kurul, bu "en kısa süre" ifadesini bir kararıyla somutlaştırmıştır: veri sorumlusu ihlali öğrendiği andan itibaren gecikmeksizin ve en geç **72 saat** içinde Kurula bildirimde bulunmalıdır. Etkilenen kişilere bildirim ise ihlalden etkilenenler tespit edildikten sonra en kısa makul sürede yapılır. Bildirimler için Kurul'un hazırladığı bildirim formu kullanılır. Bildirimin ayrıntıları ve güncel kurallar için Kurumun resmî duyuruları esas alınır.

Bu kısa süre, Modül 8'deki hazırlığın neden önemli olduğunu gösterir: "Kişisel veri etkilendi mi, kimler, hangi veri türleri?" soruları hızla cevaplanabilmeli, kimin karar vereceği önceden belli olmalıdır. İhlalin olguları, etkileri ve alınan önlemler kayıt altında tutulur.

AB'deki kişilere mal ya da hizmet sunan Türk şirketleri, Avrupa Birliği Genel Veri Koruma Tüzüğü'ne (GDPR) de tabi olabilir. GDPR'da da denetim otoritesine bildirim için, ihlalin fark edilmesinden itibaren 72 saatlik süre öngörülür.

Kamu kurumları ve kritik altyapı işletmecileri için siber güvenliğe özel ek düzenlemeler de vardır. Böyle bir kurumda çalışıyorsan, hangi düzenlemelere tabi olduğunu hukuk ve bilgi güvenliği birimlerinden öğren.

Güvenlik kültürü

Standartlar ve yasalar çerçeveyi çizer; günlük güvenliği ise insanların davranışı belirler. **Güvenlik kültürü**, bir kurumda çalışanların güvenliği başkasının işi değil, kendi işlerinin doğal parçası olarak görmesidir.

Güçlü bir güvenlik kültürünün işaretleri:

- **Bildirim cezalandırılmaz.** Şüpheli e-postaya tıkladığını hemen bildiren çalışan teşekkür alır. Bildirim cezalandırılırsa insanlar hatalarını saklar ve olaylar geç fark edilir.
- **Yönetim örnek olur.** Üst yöneticiler de MFA kullanır, kurallara istisna istemez. "Genel müdürün hesabı için MFA kapatılsın" talebi, saldırganların en çok sevdiği istisnadır.
- **Kurallar uygulanabilir.** İş imkânsız hâle getiren kurallar, çalışanları gizli yollar bulmaya iter. Güvenlik ekibi, iş birimleriyle konuşarak işi kolaylaştıran güvenli yollar sunar.
- **Farkındalık sürekli ve kısadır.** Yılda bir uzun sunum yerine, kısa ve düzenli eğitimler, gerçek örnekler ve ortalama farkındalık tatbikatları.
- **Ölçülür.** Şüpheli e-posta bildirim sayısı, eğitim tamamlama oranı, ortalama tatbikatlarında bildirim oranı gibi göstergeler izlenir.

Örnek vaka: e-ticaret mağazasında müşteri verisi sızıntısı

Bursa'daki 12 kişilik e-ticaret mağazası, bir cuma akşamı müşterilerinden birinin, kendisine mağaza adına sahte bir indirim SMS'i geldiğini ve mesajda adının ve son siparişinin yazdığını bildirmesiyle durumu fark eder.

1. **Tespit:** Bilgi işlem sorumlusu ve dış destek firması, yönetim panelinde şüpheli bir girişi inceler. Bir çalışanın, başka bir sitede sızan parolasıyla ve MFA olmadan panele giriş yapıldığı, sipariş listesinin dışa aktarıldığı görülür.

2. **Sınırlama:** İlgili hesap kilitlenir, bütün panel kullanıcılarının parolaları sıfırlanır ve panelde MFA zorunlu hâle getirilir.
3. **Kapsam:** Dışa aktarılan listede yaklaşık 3.000 müşterinin adı, telefonu, teslimat adresi ve sipariş bilgisi vardır; kart bilgisi yoktur, çünkü ödemeler bir ödeme kuruluşu üzerinden alınmaktadır.
4. **Bildirim:** Şirket sahibi, hukuk danışmanı ile birlikte, ihlali öğrendikleri andan itibaren 72 saat içinde Kurul'a bildirim yapar. Etkilenen müşterilere sade bir dille ne olduğunu, hangi verilerin etkilendiğini, şirketin ne yaptığını ve sahte mesajlara karşı nelere dikkat etmeleri gerektiğini anlatan bir bilgilendirme gönderilir.
5. **Ders çıkarma:** Bütün sistemlerde MFA, panelde toplu dışa aktarma için yönetici onayı ve olağan dışı dışa aktarmalar için uyarı kuralı devreye alınır. Kişisel veri envanteri güncellenir.

Parola tekrarı (Modül 3), eksik izleme (Modül 7), olay müdahalesi (Modül 8) ve yasal bildirim burada tek bir olayın parçalarıdır.

Sık yapılan hatalar

- **ISO/IEC 27001'i bir belge alma projesi olarak görmek.** Belge, işleyen bir yönetim sisteminin sonucu olmalıdır.
- **Kapsamı yalnız bilgi işlemle sınırlamak.** İnsan kaynakları, satın alma, hukuk ve iş birimleri de BGYS'nin parçasıdır.
- **Veri ihlalini "küçük" diye bildirmemek.** Bildirim yükümlülüğü ve süreleri, ihlali öğrenme anından itibaren işler.
- **Veri işleyenle sözleşmede güvenlik yükümlülüklerini yazmamak.** Sorumluluk veri sorumlusunda da kalır.
- **Farkındalık eğitimini yılda bir uzun sunuma indirgemek.**
- **Bildiren çalışanı suçlamak.** Bir sonraki olay saklanır.

Kendini dene

1. ISO/IEC 27001 hangi yönetim sisteminin şartlarını tanımlar?
2. Uygulanabilirlik Bildirgesi neyi gösterir?
3. KVKK'ya göre veri sorumlusu ile veri işleyen arasındaki fark nedir?
4. Kişisel Verileri Koruma Kurulu'nun kararına göre veri ihlali Kurul'a en geç ne kadar sürede bildirilmelidir?
5. Güçlü bir güvenlik kültürünün iki işaretini say.

Kendini dene cevapları

Modül 1: 1) Bütünlük. 2) Zafiyettir; tehdit, bu zafiyetten yararlanabilecek kişi ya da olaydır. 3) 12. 4) Riski aktarmak. 5) Birbirini tamamlayan birden fazla güvenlik katmanı kullanmak; biri aşılırsa diğerinin saldırıyı durdurması ya da fark etmesi.

Modül 2: 1) Solucan (worm). 2) Dışarı çıkarılan verinin yayımlanması tehdidini, yani veri sızıntısını. 3) Sesli oltalama (vishing). 4) Değişikliği uygulamadan önce tedarikçiyi önceden kayıtlı bir telefon numarasından arayarak teyit etmek ve durumu bildirmek. 5) Erişilebilirlik.

Modül 3: 1) Kimlik doğrulama kişinin iddia ettiği kişi olduğunu kontrol eder; yetkilendirme içeri girdikten sonra neleri yapabileceğini belirler. 2) Kimlik bilgisi doldurma (credential stuffing). 3) İkisi de aynı faktör türündendir (bildiğin bir şey). 4) Onaylamaz, reddeder, parolasını değiştirir ve bilgi işleme bildirir. 5) Eski rolün yetkilerinin kaldırılması.

Modül 4: 1) Açıkça izin verilmeyen bütün trafiğin engellenmesi. 2) Zararın ağır bir bölümünde kalması, bütün sistemlere yayılmaması. 3) VPN trafiği şifreler ama bağlanan kimliğini garanti etmez; çalınmış bir parolayla bağlanan saldırganı MFA durdurur. 4) WPA2 ve tercihen WPA3. 5) Ağın içinde olmasını tek başına güven sebebi saymaz; her erişimde kimliği, cihazı ve bağlamı yeniden doğrular.

Modül 5: 1) Yalnız bilinen dosya imzalarına değil davranışa bakar; şüpheli hareketi tespit eder, kaydeder ve cihazı yalıtabilir. 2) Disk şifreleme. 3) Alan adının taklit edildiği e-posta sahteciliği (oltalama ve iş e-postası dolandırıcılığı). 4) Sıfırıncı gün (zero-day) açığı. 5) İnternete açık sistemler, aktif olarak istismar edildiği bilinen açıklar ve kritik dereceli açıklar.

Modül 6: 1) Üç kopya veri, iki farklı ortam, bir kopyanın başka bir konumda olması. 2) Belirlenen süre dolmadan yönetici yetkisiyle bile silinemez ya da değiştirilemez; ağı ele geçiren saldırgan bu yedeğe dokunamaz. 3) RPO kabul edilebilir en fazla veri kaybı süresidir; RTO sistemin en geç ne kadar sürede yeniden çalışması gerektiğidir. 4) Silinen ya da şifrelenen dosyalar eşitlemeyle bulut kopyasına da taşınır. 5) "Bu süreç durursa bir saat, bir gün, bir hafta sonra ne olur?"

Modül 7: 1) Farklı kaynaklardan gelen, tek başına önemsiz görünen olayları birleştirerek anlamlı bir saldırı örüntüsünü ortaya çıkarır. 2) Farklı sistemlerin logları yan yana konduğunda olayların doğru sırası ancak saatler eşitse anlaşılabilir. 3) Yanlış pozitif zararsız bir duruma alarm üretilmesidir; yanlış negatif gerçek bir saldırıda alarm üretilmemesidir. Yanlış negatif daha tehlikelidir. 4) Gelen alarmların triyajını yapmak, yanlış pozitifleri ayıklamak ve şüpheli olayları üst kademeye aktarmak. 5) Gelen postaları dış bir adrese yönlendiren kural oluşturulması.

Modül 8: 1) Hazırlık, tespit ve analiz, sınırlama, temizleme, kurtarma, ders çıkarma. 2) Kapatmak bellekteki delilleri yok edebilir; ağdan ayırmak yayılmayı durdururken delili korur. 3) Kimin hangi delili ne zaman aldığını, nerede ve nasıl sakladığını. 4) Kapatılmazsa saldırgan aynı yoldan geri döner. 5) Suçlu bulmak değil; neyin iyi, neyin kötü işlediğini görüp sorumlu ve son tarihi belli iyileştirmeler belirlemek.

Modül 9: 1) Sistem sahibinin yazılı izni, belirlenmiş kapsam, bulguların yalnız sistem sahibine raporlanması ve verilerin korunması. 2) Zafiyet taraması otomatik olarak bilinen açıkları listeler; sızma testinde uzman, açıkların gerçekten kullanılabilir olup olmadığını kontrollü biçimde

doğrular. 3) Gri kutu testi. 4) Örneğin kapsamdaki ve kapsam dışı sistemler, test tarihleri, yasak yöntemler, acil durumda aranacak kişiler. 5) Açığı kullanmaz, kimseyle paylaşmaz, kurumun güvenlik iletişim kanalından bildirir ve kapatılması için makul süre tanır.

Modül 10: 1) Bilgi güvenliği yönetim sistemi (BGYS). 2) Ek A'daki kontrollerden hangilerinin uygulandığını ve uygulanmayanların neden uygulanmadığını. 3) Veri sorumlusu verinin neden ve nasıl işleneceğine karar verir; veri işleyen, veri sorumlusunun verdiği yetkiyle onun adına veri işler. 4) İhlalin öğrenilmesinden itibaren en geç 72 saat. 5) Örneğin bildirimin cezalandırılmaması ve yönetimin kurallara uyarak örnek olması.

Sözlük

Angajman kuralları: Sızma testinin kapsamını, zamanını, yöntemlerini ve iletişim kurallarını belirleyen yazılı belge.

Ayrıcalıklı hesap: Sistem yöneticisi gibi geniş yetkileri olan hesap.

BGYS (bilgi güvenliği yönetim sistemi): Bilgi güvenliği risklerinin sistemli biçimde yönetilmesini sağlayan politika, süreç ve kontroller bütünü.

Botnet: Ele geçirilmiş cihazların bir merkezden yönetilen ağı.

Bütünlük: Bilginin doğru, eksiksiz ve izinsiz değiştirilmemiş olması.

CVE: Bilinen güvenlik açıklarına verilen ortak tanımlayıcı numara.

CVSS: Güvenlik açıklarının ciddiyetini 0 ile 10 arasında puanlayan ortak sistem.

DDoS: Çok sayıda cihazdan gelen yoğun trafikle bir hizmeti erişilemez hâle getirme saldırısı.

Delil zinciri: Delilin kim tarafından, ne zaman alındığını ve nasıl saklandığını gösteren kayıt.

Derinlemesine savunma: Birbirini tamamlayan birden fazla güvenlik katmanı kullanma yaklaşımı.

DMARC, DKIM, SPF: Bir alan adı adına gönderilen e-postaların doğrulanmasını sağlayan ve sahteciliği zorlaştıran DNS kayıtları.

EDR: Uç noktadaki şüpheli davranışları tespit eden, kaydeden ve müdahale imkânı veren güvenlik aracı.

En az yetki ilkesi: Kullanıcıya ve sisteme işini yapması için gereken en az erişimin verilmesi.

Erişilebilirlik: Yetkili kişinin bilgiye ve sisteme ihtiyaç duyduğu anda ulaşabilmesi.

Fidye yazılımı: Dosyaları ya da sistemleri şifreleyip açılması için fidye isteyen zararlı yazılım.

Gizlilik: Bilginin yalnız görmeye yetkili kişilerce görülebilmesi.

Güvenlik duvarı: Ağlar arasındaki trafiği kurallara göre izin veren ya da engelleyen sistem.

Güvenlik olayı: Bilginin gizliliğini, bütünlüğünü ya da erişilebilirliğini bozan veya bozma tehdidi taşıyan, müdahale gerektiren durum.

İş e-postası dolandırıcılığı (BEC): Yönetici ya da tedarikçi taklidiyle sahte ödeme yaptırmaya yönelik e-posta dolandırıcılığı.

Kimlik bilgisi doldurma: Bir yerden sızan kullanıcı adı ve parolaların başka sistemlerde otomatik olarak denenmesi.

Log: Bir sistemin yaptığı işlemleri zaman damgasıyla kaydettiği satırlar.

MFA (çok faktörlü kimlik doğrulama): Oturum açarken farklı türden en az iki kanıt istenmesi.

Oltaama: Sahte mesajla kişiyi bilgi vermeye, dosya açmaya ya da ödeme yapmaya kandırma girişimi.

Risk: Bir tehdidin bir zafiyeti kullanarak bir varlığa zarar verme ihtimali ve zararın büyüklüğü.

RPO: Kabul edilebilir en fazla veri kaybı süresi.

RTO: Bir sistemin en geç ne kadar sürede yeniden çalışması gerektiğini gösteren hedef süre.

Segmentasyon: Ağı birbirinden ayrılmış bölümlere bölüp aralarındaki trafiği sınırlamak.

SIEM: Farklı kaynaklardan gelen logları toplayan, ilişkilendiren ve alarm üreten sistem.

Sıfır güven: Ağın içinde olmayı güven sebebi saymayan, her erişimi yeniden doğrulayan güvenlik yaklaşımı.

Sıfırıncı gün açığı: Henüz yaması bulunmayan ve saldırganlarca kullanılan güvenlik açığı.

Sızma testi: Yazılı izinle ve belirli kapsamda, açıkların gerçekten kullanılabilir olup olmadığının uzman tarafından doğrulandığı test.

SOC: Kurumun sistemlerini sürekli izleyen ve olaylara ilk müdahaleyi yapan güvenlik operasyon merkezi.

Sosyal mühendislik: İnsanların güvenini, merakını ya da korkusunu kullanarak bilgi ya da erişim elde etme yöntemi.

Tehdit: Bir varlığa zarar verebilecek olası olay ya da kişi.

Triyaj: Gelen alarmların incelenip gerçek olup olmadığına ve aciliyetine karar verilmesi.

Uygulanabilirlik Bildirgesi: ISO/IEC 27001'de hangi kontrollerin uygulandığını ve uygulanmayanların gerekçesini gösteren belge.

Uç nokta: Bilgisayar, telefon, tablet gibi kullanıcının doğrudan çalıştığı cihaz.

VPN: İnternet üzerinden iki nokta arasında şifreli bağlantı kuran sanal özel ağ.

Yama: Yazılımdaki bir açığı ya da hatayı kapatan güncelleme.

Zafiyet: Bir tehdidin yararlanabileceği zayıf nokta.

Sonraki adım

Eğitimi bitirdiysen bilgini ölç. Daphne Kariyer'de bu eğitimin konularıyla ilgili şu testler ücretsizdir: Siber Güvenlik, Bilgi Güvenliği, Ağ Güvenliği, SOC Analistliği, Siber Olay Müdahalesi ve ISO 27001 Bilgi Güvenliği. Her test 20 sorudan oluşur. 55 ve üzeri puan alırsan isteğe bağlı olarak doğrulanabilir dijital sertifika alabilirsin.

Önce Siber Güvenlik ve Bilgi Güvenliği testleriyle başlayıp ilgi alanına göre diğerlerine geçebilirsin. Sonucu düşük çıkan bir testte ilgili modüle dönüp tekrar oku.

daphnekariyer.com/dijital-yetkinlikler/