

Güvenlik En İyi Uygulamaları

Günümüzün bağlantılı cihazlarla dolu dünyasında bu hususlar ve ortak kaygılar doğaldır. Bunların farkında olmak ilk adımdır. Bir sonraki adım ise bu makul en iyi uygulamaları, bağlantılı tüm cihazlarınıza uygulamaktır. Bu kontrol listesini bir planlama kılavuzu olarak kullanın.

1. Erken Başla

Gelecek teknolojileri ve bunu nasıl koruyacağınızı planlayın.

2. Verileri Korumak

Mümkün olduğu her durumda şifreli ve kimlik doğrulamalı bağlantılar kullanın.

3. Kontrol Hizmetleri

Kullanmayacağınızı düşündüğünüz teknoloji hizmetlerini kapatmayı değerlendirin.

4. Şifreleri Değiştirin

Varsayılan şifreleri kullanmak, bilgisayar korsanlarının cihazlara erişmesini kolaylaştırır. **Kullanıcı Arayüzü Şifrelerini Etkinleştirin.**

5. Uzaktan Yönetim

Ayarları hızlı bir şekilde güncellenize olanak vermesi için güvenli bir uzaktan yönetim sistemi kullanın. Cihazlar, çözümler ve sistemler eski ayarlarla ne kadar uzun süre kullanılırlarsa o kadar kolay hedef olurlar.

6. Etkinlik Günlüğünü Etkinleştirin

Kötü davranışları tespit etmek için mümkün olduğunda etkinlik ve denetim günlüklerini kullanın.

7. Bilmesi Gerekenler

Güncelleme programlarını ve planlarını yalnızca bilmesi gerekenlere verin. Güncelleme planları hakkında çok sayıda çalışan bilgi sahibi olduğunda, güvenlik ihlalleri olasılığı artar.

8. OOT (Ulaşılamayan) Cihazları İzleme

Sisteminizi "ulaşılamayan" cihazlar için sürekli olarak izlemeye yönelik bir yöntem geliştirin. Bir cihazın kaldırıldığından şüphelendiğinizde, konumunu teyit eden kadar kimlik bilgilerini geri çekin.

9. Güncellenebilirlik

Yeni standartlarla güncel kalmak için uzun ömürleri boyunca güncellenebilen cihazlar seçin. Güncelleme sistemlerinin güncelleme dosyalarıyla oynanmasını önleyebildiğinden emin olun.

10. Cihaz Emekliliği

Cihaz emekliliğini planlamak için, kurumsal sistem ayarlarını kaldırın, cihaz kullanıcı hesaplarını/kimlik bilgilerini silin ve mevcut sistemlerin emekli birimleri aramak üzere kodlanmadığından emin olun.

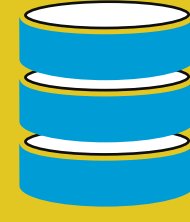
11. CIA (Gizlilik Bütünlük Kullanılabilirlik)

Cihazın kullanım ömrünün tüm aşamalarında "Gizlilik", "Bütünlük" ve "Kullanılabilirlik" hususlarını dikkate alın.

12. Sürekli Planlama

Güvenlik uygulamalarındaki güncellemeler sürekli bir öncelik olmalıdır. Güvenlik planlaması bir kerelik bir olay değildir.

Biliyor muydunuz?



\$360.000

Şifreleme, veri ihlali maliyetlerini ortalama **\$360.000** azaltmasıyla en etkili saldırı önlemidir.¹



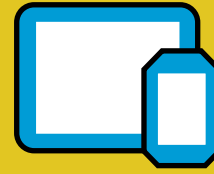
%81

Zayıf veya çalıntı şifre kullanılması bilgisayar korsanlığı bağlantılı veri ihlallerinin **% 81'ini oluşturmaktadır.**²



\$1,2 milyon

Veri ihlali olay müdahale ekipleri ve test yanıt planları olan şirketler bir veri ihlali maliyetini **\$1,2 milyondan fazla düşürür.**³



Tüketicilerin %38'i

Firmaların **%38'i** kurumsal cihazlarla ilgili güvenlik olayları bildirdi.⁴



%40

%40 siber saldırıların bir faktör olduğunu söylüyor ve bu da mobil cihaz güvenliğini daha da önemli kılıyor.



197 Gün

Bir kuruluşta bir veri ihlalinin gerçekleştiğinin farkına varılması ortalama **197 gün** alıyor.⁵

¹ Cost of a Data Breach Report 2019, IBM Security • ² 2017 Verizon Data Breach Investigations Report, IBM Security • ³ Cost of a Data Breach Report 2019 • ⁴ Carbon Black Incident Response Threat Report, November 2018 • ⁵ 2018 ve 2019 Cost of Data Breach, Ponemon Institute

ACCESS DENIED
ACCESS DENIED
ACCESS DENIED
ACCESS DENIED