TR CYBERSECURITY ALLIANCE

Siber Hijyende En İyi 10 Uygulama

GİRİŞ

Dijitalleşmenin hızla ilerlediği günümüzde, siber tehditler sadece büyük organizasyonlar için değil, bireyler ve küçük işletmeler için de ciddi bir risk oluşturmaktadır. Siber hijyen, bu tehditlere karşı alınabilecek önleyici tedbirlerin temelini oluşturur ve güvenliğin sürdürülebilir hale gelmesinde kritik bir rol oynar. Bu belge 21 Kasım 2024 tarihinde gerçekleşen TR Cybersecurity Alliance çalıştayı sonucunda hazırlanmış olup, siber hijyen alanında uygulanabilecek en iyi 10 yöntemi kapsamaktadır. Amaç, bireylerden kurumlara kadar herkesin dijital varlıklarını daha güvenli bir şekilde yönetmesini ve korunmasını sağlamak için yol göstermektir.

1. Varlıklarınızı Bilin ve Yönetin

Siber güvenliğin ilk adımı her zaman varlık yönetimidir. Bir sistemde yer alan sunucu, istemci, ağ cihazı, güvenlik duvarı, veri tabanı, IoT veya yönetilemeyen tüm cihazları otomatik keşfedecek yöntemler kullanın. Varlıklarınızın iş risklerini belirleyin ve risk seviyesine göre varlıklarda oluşacak değişiklikleri veya olayları izleyin.

2. Bilişim Sisteminizi Sıkılaştırın

Bilişim sisteminde bulunan her varlığa güvenlik sıkılaştırması uygulayın. Güvenlik sıkılaştırması tüm varlıkların güvenli konfigürasyonlara sahip olması ve zafiyetlerinin izlenerek yamalarının yüklenmesi süreçlerini kapsar. Güvenli konfigürasyonlar için CIS Benchmark veya CBDDO tarafından yayınlanan Bilgi ve İletişim Güvenliği Rehberi belgelerini kullanın.

3. Güçlü Parola Politikaları Uygulayın ve Şifre Kasası Kullanın

Çalışanlar ve sistem yöneticileri için güçlü ve karmaşık parolalar belirlemelerini zorunlu kılın. Parolalar en az 12 karakter uzunluğunda olmalı, büyük ve küçük harfler, rakamlar ve semboller içermelidir. Ayrıca, parola yönetim ve şifre kasası araçları kullanarak parolaların gizliliğini koruyun ve mümkün olan en kısa sürede güncellenmesini sağlayın. Kurallara uygun erişimlerin tamamını denetleyecek mekanizmaları çalıştırın.

4. Çok Faktörlü Kimlik Doğrulama (MFA) Kullanın

Mümkünse tüm bilişim sistemlerinde çok faktörlü kimlik doğrulama (MFA) uygulayın. Çok faktörlü kimlik doğrulama, kritik veya internete açık sistemlerin yalnızca parolalarla değil, ek güvenlik önlemleriyle de korunmasını sağlar.

5. Veriyi Şifreleyin

Şifrelenmemiş veri güvenliği değildir. Kritik veriler, önemli veriler, özellikle finansal, kişisel ve sağlık bilgileri şifrelenerek saklanmalı ve iletilmelidir.

6. 3-2-1-0 Prensibi ile Yedekleme Yapın

En az 3 kopya yedek, en az 2 farklı medya, en az 1 çevrimdışı yedek, 0 hatalı yedekleme ve geri dönüş prensibi ile yedekleme sistemini güvenilir kılın.

7. Temel Koruma Ürünlerini Kullanın

Siber ataklardan koruma sağlayacak güvenlik duvarı, antivirüs, EDR, Host IPS, Web Gateway, Email Gateway gibi ürünleri kullanın. Bu ürünlerin konfigürasyonlarını düzenli kontrol edin ve güncel olduklarından emin olun.

8. Eğitim ve Farkındalık Programları Düzenleyin

Şirket personellerini olası siber tehditler ve kimlik avı saldırıları konusunda sürekli eğitin. Oltalama simülatörleri ve eğitim portalları kullanarak süreçleri otomatikleştirin. Farkındalığı yüksek personeli ödüllendirin.

9. Sızma Testi ve Atak Simülasyonu Yapın

Siber güvenlik sisteminin kalitesini ölçmek ve olası hataları siber saldırılardan önce tespit edebilmek için düzenli olarak Sızma Testi ve Atak Simülasyonu yapın. Bu çalışmalar sistem yöneticilerinden habersiz, beklenmedik anlarda ve düzenli olarak yapılmalıdır.

10. Siber Olay Müdahale Planı Oluşturun

Siber olay sayısını sıfırlamak imkansızdır. Bir siber saldırı durumunda hızlı ve etkili bir şekilde yanıt verebilmek için bir siber olay müdahale planı oluşturun. Plan, acil durumlar için prosedürler, iletişim yolları ve sorumlulukları içermelidir. Ayrıca, olay sonrası bir inceleme yaparak gelecekteki tehditlere karşı daha iyi hazırlıklı olun.

Siber hijyen, etkili bir siber güvenlik stratejisinin temel taşlarından biridir ve günlük alışkanlıkların güvenlik süreçlerine entegre edilmesiyle başlar. Bu dokümanda sunulan 10 uygulama, siber saldırılara karşı güçlü bir savunma mekanizması oluşturmanın yanı sıra, organizasyonel güvenliği sürdürülebilir kılma konusunda rehberlik etmektedir. TR Cybersecurity Alliance olarak, dijital dünyada güvenliği artırmak için en iyi uygulamaları paylaşmaya devam edecek ve toplulukları bu alanda bilinçlendirme misyonumuzu sürdüreceğiz. Unutulmamalıdır ki, siber hijyen sadece bir seçim değil, dijital çağın vazgeçilmez bir gerekliliğidir.

Çalışmaya Katkıda Bulunanlar

Ahmet Özkan
Ahmet Öztoprak
Ali Tursun
Alper Sulan
Asım Yıldız
Caner Dağlı
Deniz Şener
Ekrem Kolday
Gökhan Ilgıt
İlker Çağrı Güven
Kayıhan Altınöz
Murat Zaralı
Nusret Karakaya
Onur Mutlu İmamoğlu
Ömer Çuhadaroğlu
Özgür Orhan
Serkan Akcan
Tuncay Arslan