KURUMLARDA SİBER GÜVENLİK

**Kurumlarda Siber Güvenlik Nasıl Sağlanır?**

Siber güvenlik, modern iş dünyasının temel bir gerekliliğidir. Kurumlar, siber saldırıların artması ve veri ihlallerinin ciddiyeti göz önüne alındığında, güvenlik önlemleri almaksızın faaliyet gösteremezler. İşte kurumlarda siber güvenliği sağlamanın ayrıntılı bir kılavuzu:

**1. Siber Güvenlik Politikaları ve Eğitimi:**

* Kurum içi siber güvenlik politikaları belirlemek kritiktir. Bu politikalar, çalışanların ve yöneticilerin siber güvenlik konularında nasıl hareket etmeleri gerektiğini tanımlamalıdır.
* Tüm çalışanlara düzenli olarak siber güvenlik eğitimi verilmelidir. Bu eğitimler, güçlü şifreler oluşturma, phishing saldırılarını tanıma ve güvenli internet kullanımı gibi konuları içermelidir.

**2. Ağ Güvenliği:**

* Güvenlik duvarları (firewall) kullanılmalı ve bu güvenlik duvarları düzenli olarak güncellenmelidir.
* Ağ izleme ve saldırı tespiti sistemleri, ağ trafiği üzerinde anormallikleri tespit ederek potansiyel saldırılara karşı önlem alır.

**3. Veri Koruma ve Şifreleme:**

* Hassas veriler, hem depolama hem de iletim sırasında şifrelenmelidir. Kullanılan şifreleme algoritmaları güncel ve güvenli olmalıdır.
* Verilerin sızdırılmasını engellemek için veri kayıtlarının düzenli olarak denetlenmesi gerekir.

**4. Güncel Yazılımlar ve Sistemler:**

* İşletim sistemleri ve yazılımlar düzenli olarak güncellenmelidir. Güvenlik yamaları hızla uygulanmalıdır.
* Yazılım kaynakları güvenilir ve resmi kaynaklardan indirilmelidir.

**5. Güçlü Kimlik Doğrulama:**

* Çift faktörlü kimlik doğrulama (2FA) gibi güçlü kimlik doğrulama yöntemleri kullanılmalıdır. Bu, yetkisiz erişim riskini azaltır.

**6. Veri Yedekleme ve Kurtarma:**

* Veri yedekleme stratejileri oluşturulmalıdır. Veri kaybı durumunda, hızlı bir veri kurtarma planı uygulanmalıdır.

**7. Güvenlik İzleme ve İncelenmesi:**

* Ağ trafiği ve sistem günlükleri düzenli olarak izlenmeli ve incelenmelidir. Potansiyel saldırılar veya güvenlik ihlalleri hızlı bir şekilde tespit edilmelidir.

**8. Güvenlik Yazılım ve Araçları:**

* Antivirüs yazılımı, kötü amaçlı yazılım tespiti ve saldırı önleme araçları gibi güvenlik yazılımları kullanılmalıdır.

**9. Yetkilendirme ve Erişim Kontrolü:**

- Çalışanların sadece gereksinim duydukları kaynaklara ve verilere erişimleri sağlanmalıdır. İşlevlere göre yetkilendirmeler yapılmalıdır.

**10. Acil Durum Planları:**

- Siber güvenlik ihlali durumunda nasıl bir tepki verileceği ve nasıl bir acil durum planının uygulanacağı önceden belirlenmelidir.

**11. Dış Tehdit İzleme:**

- Kurumlar, dış tehditleri izlemek ve bunlara karşı savunma stratejileri geliştirmek için siber güvenlik firmaları veya hizmetleri ile işbirliği yapabilirler.

**12. Yasal Uyumluluk:**

- Kurumlar, siber güvenlikle ilgili yasalara ve endüstri standartlarına uyum sağlamalıdır.

Bu ayrıntılı önlemler, kurumların siber güvenliklerini sağlama konusunda yardımcı olurken, her kurumun kendi gereksinimlerine ve tehditlerine uygun stratejiler geliştirmesi önemlidir.

- Kullanıcılar ile ilgili faaliyetler neler olmalı?

1. **Kimlik Doğrulama ve Yetkilendirme:**
   * Kullanıcıların kimlikleri doğrulanmalı ve yalnızca gerektiğinde belirli kaynaklara erişim izni verilmelidir.
   * Güçlü parola politikaları oluşturulmalı ve düzenli olarak parola değişikliği teşvik edilmelidir. Çift faktörlü kimlik doğrulama (2FA) kullanımı önerilir.
2. **Veri Erişimi Kontrolü:**
   * Kullanıcıların erişebileceği veriler sınıflandırılmalıdır. Hassas verilere sadece gereksinim duyan kişilerin erişimi sağlanmalıdır.
3. **Eğitim ve Farkındalık:**
   * Kullanıcılar, siber güvenlik tehditlerini tanımaları ve nasıl tepki vermeleri gerektiği konusunda eğitilmelidir. Bu eğitimler, phishing saldırılarına karşı dikkatli olma ve güvenli internet kullanma konularını içerebilir.
4. **Kullanıcı Faaliyet İzleme:**
   * Kullanıcıların faaliyetleri düzenli olarak izlenmelidir. Bu izleme, anormal aktiviteleri tespit etmeye yardımcı olabilir ve potansiyel tehditleri önceden belirlemeye yardımcı olur.
5. **Veri Paylaşımı ve USB Kullanımı Kontrolü:**
   * Veri paylaşımı ve USB kullanımı sınırlamaları belirlenmelidir. Bilinmeyen kaynaklardan USB cihazlarına veri aktarımı engellenebilir.
6. **Erişim Denetimleri:**
   * Kullanıcıların erişim aktiviteleri izlenmeli ve denetlenmelidir. Anomali tespiti için otomatik sistemler kullanılabilir.
7. **Güncel Yazılım ve Sistemler:**
   * Kullanıcıların işletim sistemleri ve yazılımları güncel tutmaları teşvik edilmelidir. Güncellemeler, güvenlik açıklarının kapatılmasına yardımcı olur.
8. **Mobil Cihaz Yönetimi (MDM):**
   * Kurum içi veya BYOD (Kendi Cihazını Getir) politikaları, mobil cihazların güvenliğini sağlamak için kullanılabilir. MDM yazılımı kullanarak cihazları yönetmek ve izlemek mümkündür.
9. **Çalışan Ayrılıkları:**
   * Çalışanların işten ayrılması veya görev değişikliği durumunda erişim hakları hızla gözden geçirilmelidir. Erişim hakları anında iptal edilmelidir.
10. **Acil Durum Hazırlıkları:**
    * Kullanıcılar, siber güvenlik olaylarına nasıl tepki vereceklerini bilmelidir. Acil durum planları, kullanıcılara rehberlik eder.
11. **Şüpheli Faaliyet Raporlama:**
    * Kullanıcılar, şüpheli faaliyetleri veya güvenlik ihlallerini hızlı bir şekilde rapor etmeli ve bu raporlar ciddiye alınmalıdır.

Kullanıcılar, siber güvenlik savunmasının önemli bir parçasıdır ve bu nedenle siber güvenlik stratejilerinin bir parçası olarak düşünülmelidir. Bilinçli, eğitimli ve dikkatli kullanıcılar, potansiyel tehditlere karşı daha etkili bir savunma sağlarlar.