

KURUMSAL
SİBER GÜVENLİK
ÖNLEMLERİ

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

USOM
ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ

Özel sektörde faaliyetlerini yürüten şirket, vakıf ve okul gibi kuruluşlara yönelik siber güvenlik tehditleri, diğer alanlardaki kuruluşlara göre farklılık göstermektedir. Esas olarak kurumsal organizasyon yapısındaki her kuruluşun tolerans seviyelerine göre özelleştirilmiş güvenlik politikaları geliştirerek uygulaması en faydalı savunma tedbiri olacaktır. Ancak müteakip maddelerde belirtilen önlemlerin alınması her kuruluşa faydalı olacaktır.



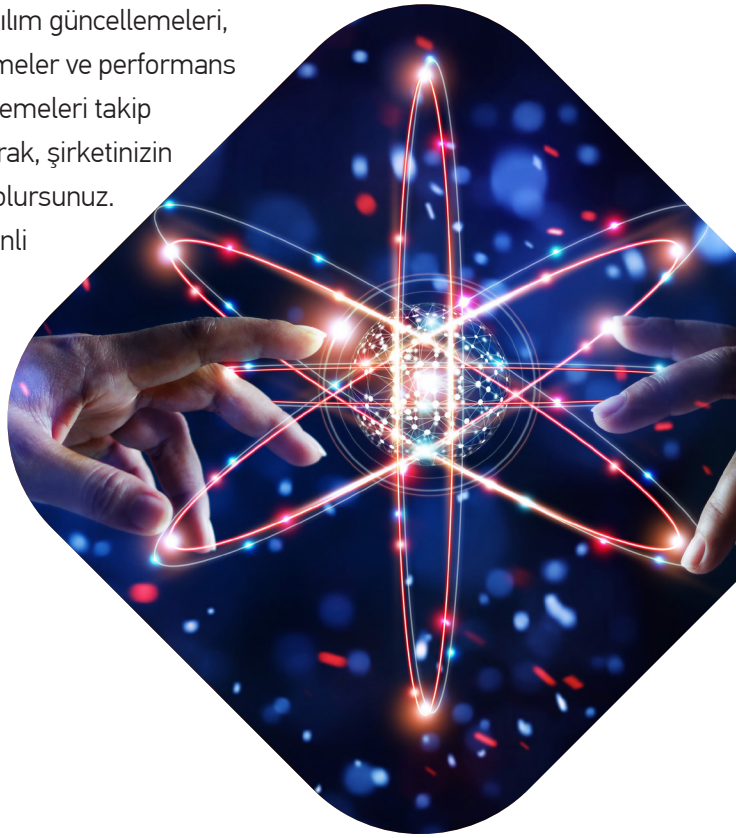
01 **Güçlü parola politikaları uygulayın:** Güçlü parola politikaları, çalışanların güvenliğini artırmak için önemli bir adımdır. Çalışanlarınızı güçlü ve benzersiz parolalar kullanmaya teşvik etmek, hesaplarının saldırılara karşı daha korunaklı hale gelmesini sağlar. Güçlü parolalar, tahmin edilmesi zor ve karmaşık kombinasyonlardan oluşmalıdır. Ayrıca, düzenli parola değişiklikleri yapılması, olası saldırılara karşı ek bir önlem sağlar. Bu politikaların uygulanması, şirketinizin siber güvenlik savunmasını güçlendirir ve çalışanlarınızın hassas bilgilerin güvenliğini sağlamasına yardımcı olur.



02 **İki faktörlü kimlik doğrulamayı zorunlu kılın:** İki faktörlü kimlik doğrulama, çalışanların hesaplarını ek bir güvenlik katmanıyla korumak için kullanılan bir yöntemdir. Bu yöntemde, kullanıcılar sadece parolalarını değil, aynı zamanda ikinci bir doğrulama faktörünü de sağlamak zorundadır, örneğin bir SMS doğrulama kodu veya bir doğrulama uygulaması tarafından üretilen bir zaman tabanlı kod kullanılabilir. Bu ek faktör, hesapların yetkisiz erişimden korunmasını sağlar ve bir parolanın çalınması durumunda bile hesap güvenliğini artırır. İki faktörlü kimlik doğrulama, siber saldırganların hesaplara izinsiz erişimini büyük ölçüde engeller ve çalışanların hesaplarının güvenliğini sağlamak için etkili bir önlemdir. İşyerlerinde bu yöntemin zorunlu hale getirilmesi, hesaplar üzerindeki potansiyel tehditleri azaltır ve veri güvenliğini önemli ölçüde artırır. Güncel güvenlik yazılımları kullanın: Antivirüs, güvenlik duvarı ve zararlı yazılım tarama araçları gibi güncel koruma yazılımlarını kullanarak sistemlerinizi koruyun.

03 **Çalışanlara siber güvenlik eğitimi verin:** Çalışanlara siber güvenlik eğitimi vermek, kuruluşunuzun güvenlik kültürünü geliştirmek ve çalışanlarınızı siber tehditlere karşı bilinçlendirmek için önemli bir adımdır. Eğitimler, çalışanlara güvenlik politikalarını, veri koruma yöntemlerini ve güvenlik tehditlerini anlamalarında yardımcı olur. Böylece, şirket içindeki her seviyeden çalışanlar, bilinçli bir şekilde güvenlik önlemlerini uygulayabilir ve olası siber saldırılara karşı daha dirençli olabilirler. Siber güvenlik eğitimi aynı zamanda sosyal mühendislik saldırıları gibi gelişmiş taktiklerin fark edilmesine ve engellenmesine yardımcı olur. Eğitim programları düzenli olarak güncellenmeli ve yeni tehditlere ve tekniklere karşı çalışanları sürekli olarak bilgilendirmelidir. Bu sayede, çalışanlarınızın siber güvenlik konusundaki bilinç düzeyi artar ve şirketinizin genel güvenliği sağlanır.
Bu kapsamda BTK Akademi tarafından etkili, ücretsiz ve sertifikalı eğitimler sağlanmaktadır. Personelinizin https://www.btkakademi.gov.tr adresinden eğitim almasını teşvik ederek bilinçlenmesini sağlayabilir, böylece kuruluşunuzun güvenliğine katkıda bulunabilirsiniz.

04 **Yazılım güncellemelerini düzenli olarak yapın:** Yazılım güncellemelerini düzenli olarak yapmak önemlidir. Güncellemeler, yazılımınızın en son sürümüne yükseltilmesini sağlar ve güvenlik açıklarını kapatır. Bu sayede, potansiyel saldırganlar tarafından kullanılabilecek zayıf noktaları en aza indirirsiniz. Yazılım güncellemeleri, yeni güvenlik önlemleri, düzeltmeler ve performans iyileştirmeleri içerebilir. Güncellemeleri takip ederek ve zamanında uygulayarak, şirketinizin siber güvenliğini güçlendirmiş olursunuz. Bu nedenle, yazılımlarınızı düzenli olarak güncellemeniz, siber saldırılara karşı koruma sağlamak için önemli bir adımdır.





05 **Veri yedeklemesi yapın:** Veri yedeklemesi, önemli verilerinizi kaybetme riskine karşı korumak için kritik bir adımdır. Bu önlem, düzenli aralıklarla verilerinizi kopyalayarak olası veri kaybını önler. Yedeklemelerinizi farklı bir depolama ortamına kaydetmek, felaket durumlarında verilere erişimi sağlar. Böylece, sistem arızaları, doğal afetler veya kötü amaçlı saldırılar gibi durumlarla karşılaştığınızda verilerinizi geri yükleyebilirsiniz. Veri yedeklemesi, iş sürekliliğini sağlamak ve veri bütünlüğünü korumak için önemli bir adımdır. Ağ trafiğini izleyin: Ağ trafiğini sürekli olarak izleyen ve anormallikleri tespit eden bir güvenlik sistemi kullanın.



06 **Zayıf noktaları tespit edin:** Zayıf noktaları tespit etmek önemli bir adımdır. Sistemlerinizde güvenlik açıkları taraması ve sızma testleri yaparak bu zayıf noktaları belirleyebilirsiniz. Güvenlik açıkları taraması, mevcut yazılım, ağ ve sistemlerdeki potansiyel güvenlik açıklarını tarayarak tespit etmeyi sağlar. Sızma testleri ise gerçek saldırı senaryolarını simüle ederek sistemlerinizi test eder ve güvenlik açıklarını gerçek bir saldırganın bakış açısıyla bulmayı hedefler. Bu testler sayesinde zayıf noktaları belirleyerek, gerekli güvenlik düzeltmelerini yapabilir ve sisteminizi güçlendirebilirsiniz. Bu, proaktif bir yaklaşım benimseyerek potansiyel saldırılara karşı korumanızı güçlendirir ve güvenlik açıklarını en aza indirir. Veri şifrelemesi kullanın: Hassas verileri şifreleyerek koruyun ve şifrelenmiş veri aktarımı için SSL/TLS protokolünü kullanın.



07 **Güvenlik politikaları ve prosedürleri belirleyin:** Şirket içinde güvenlik politikaları ve prosedürleri oluşturmak ve uygulamak önemlidir. Bu politikalar ve prosedürler, çalışanlara siber güvenlik kurallarını belirtir ve uygulanması gereken adımları tanımlar. Örneğin, parola politikaları, erişim kontrolü, veri gizliliği ve yetkilendirme gibi konuları kapsar. Bu politikaların uygulanması, güvenlik bilincini artırır, veri güvenliğini sağlar ve siber saldırılara karşı daha güçlü bir savunma mekanizması oluşturur. Güvenlik politikaları ve prosedürleri düzenli olarak gözden geçirilmeli ve güncellenmelidir, böylece değişen tehditlere uyum sağlanabilir ve sürekli olarak iyileştirilebilir.

08 Yetkilendirme ve erişim kontrollerini güçlendirin: Yetkilendirme ve erişim kontrollerini güçlendirmek, sistemlere ve verilere erişimi sınırlamayı ve gereksiz ayrıcalıkları kaldırmayı içerir. Bu, sadece yetkili kullanıcıların kritik kaynaklara erişebileceği anlamına gelir. Ayrıca, ayrıcalıkların düzenli olarak gözden geçirilerek gereksiz erişimlerin engellenmesi sağlanır. Bu önlem, yetkisiz erişim riskini azaltır ve şirket içindeki veri güvenliğini artırır. Ayrıca, çalışanlar arasında doğru yetkilendirme ve erişim politikalarının uygulanmasını sağlar.

09 Taşınabilir cihazları koruyun: Şirket içinde kullanılan taşınabilir cihazlar, güvenlik açısından önemli bir risk oluşturabilir. Bu nedenle, bu cihazlar için güvenlik önlemleri alınmalıdır. Şifreleme kullanarak cihazlardaki verilerin korunması sağlanmalı ve kaybolma durumunda uzaktan silme özelliği etkinleştirilmelidir. Böylelikle, kaybolan veya çalınan bir cihazın içerdiği verilere yetkisiz erişim engellenir ve hassas bilgilerin korunması sağlanır. Bu önlemler, şirket verilerinin güvenliğini artırır ve potansiyel risklere karşı önemli bir koruma sağlar.

10 Uygulama güvenliğine odaklanın: Yazılım şirketleri için uygulama güvenliği, önemli bir konudur. Uygulamalarınızda güvenlik açıklarını tespit etmek ve düzeltmek için düzenli güvenlik testleri yapmanız gerekmektedir. Bu testler, potansiyel zayıf noktaları ortaya çıkarır ve saldırılara karşı daha güçlü bir savunma sağlar. Uygulama güvenliğine odaklanmak, müşterilerinizin ve kullanıcıların verilerinin korunmasını sağlar ve şirketinizin itibarını güçlendirir. Düzenli güvenlik testleri, uygulamalarınızın güvenliğini sürekli olarak iyileştirmenizi sağlar ve gelecekteki saldırıları önlemek için proaktif bir yaklaşım sunar.





11 Çalışanların ayrılış süreçlerini yönetin: Çalışanların ayrılış süreçlerini yönetmek, işten ayrılan bir çalışanın hesaplarına hemen erişimi kapatmayı ve gizli bilgileri koruma politikalarını uygulamayı içerir. Bu önlem, işten ayrılan çalışanların şirket kaynaklarına yetkisiz erişimi önleyerek veri güvenliğini sağlar. Hesap erişiminin hemen kapatılması, eski çalışanların şirket verilerini kötüye kullanma riskini azaltır. Gizli bilgilerin koruma politikalarının uygulanması ise çalışanların yetkisiz veri paylaşımını önler ve şirketin ticari sırlarını korur. Çalışanların ayrılış süreçlerinin etkin bir şekilde yönetilmesi, şirketlerin siber güvenliğini güçlendirmek için kritik bir adımdır.



12 Ağınızı segmente edin: Ağınızı segmente etmek, ağınızı farklı bölümlere ayırarak izole etmek ve potansiyel saldırı durumunda saldırının yayılma riskini azaltmak anlamına gelir. Bu, farklı bölümlerin birbirinden bağımsız çalışmasını sağlayarak güvenlik seviyesini artırır. Örneğin, yönetim, çalışanlar ve misafirler için farklı ağ bölümleri oluşturarak, yetkisiz erişimi kısıtlayabilir ve iç ağa sızma riskini azaltabilirsiniz. Ağ segmentasyonu ayrıca saldırılar sırasında zararın sınırlanmasına yardımcı olur, çünkü saldırganlar bölümler arasında kolayca hareket edemezler. Bu önlem, ağ güvenliğini güçlendirir ve kritik verilerin, sistemlerin ve hizmetlerin korunmasına yardımcı olur. Veri gizliliğini sağlayın: Hassas verilerin güvenliğini sağlamak için uygun şifreleme ve erişim kontrolü önlemlerini uygulayın.



13 Harici güvenlik testlerine katılın: Harici güvenlik testlerine katılmak, şirketinizin sistemlerindeki potansiyel güvenlik zayıflıklarını tespit etmek ve düzeltme adımlarını uygulamak için önemli bir adımdır. Bu testler, yetenekli güvenlik uzmanları tarafından gerçekleştirilir ve şirketinizin savunma mekanizmalarını sınar. Test sonuçlarına dayanarak güvenlik açıkları belirlenir ve bu açıkları düzeltmek için gerekli önlemler alınır. Bu şekilde, şirketinizin siber saldırılara karşı daha güvenli hale gelmesi sağlanır ve potansiyel tehlikeler önceden engellenir.



14 Çalışanların BYOD politikasını yönetin: BYOD (Kendi Cihazını Getir) politikasının yönetilmesi, çalışanların kendi cihazlarını iş ortamında kullanmasına izin verilirken güvenlik risklerini en aza indirmek için önemlidir. Bu politika kapsamında güvenlik politikaları oluşturulmalı ve çalışanlara cihaz güvenliği konusunda bilinçlendirme eğitimi verilmelidir. Ayrıca, güvenlik önlemleri olarak cihazlara parola zorunluluğu getirilmeli, güncel yazılım güvenlik güncellemeleri yapılmalı ve veri şifrelemesi gibi önlemler alınmalıdır. BYOD politikasının etkin bir şekilde yönetilmesi, hem çalışanların cihazlarını kullanma esnekliğini sağlar hem de şirketin güvenliğini korur. Olay günlüklerini izleyin: Sistem olay günlüklerini düzenli olarak izleyin ve potansiyel saldırıları tespit etmek için olayları analiz edin.



15 Fiziksel güvenliği sağlayın: Şirketler, siber güvenliği sağlamanın yanı sıra fiziksel güvenliği de göz önünde bulundurmalıdır. Sunucu odaları ve ağ altyapısı gibi kritik alanlar, yetkisiz erişimden korunmalı ve fiziksel olarak güvence altına alınmalıdır. Bu, güvenlik önlemlerinin fiziksel engeller, güvenlik kameraları ve erişim kontrolleri gibi unsurları içermesini gerektirir. Yetkisiz kişilerin bu kritik alanlara girmesini önlemek, veri güvenliğini ve iş sürekliliğini sağlamak için önemlidir. Fiziksel güvenlik tedbirleri, şirketlerin veri merkezlerini, sunucularını ve ağ altyapısını korumak ve potansiyel tehditlere karşı savunmaya geçmek için hayati önem taşır.



16 Sosyal mühendislik saldırılarına karşı eğitin: Çalışanları sosyal mühendislik saldırılarına karşı eğitmek, onları bu tür manipülasyon taktiklerini tanımaya ve engellemeye yönlendirmenin önemli olduğunu ifade eder. Eğitim programları, çalışanların dolandırıcılık, kimlik avı ve sahtekârlık gibi sosyal mühendislik saldırılarını nasıl tanıyacaklarını ve güvenlik protokollerini nasıl izleyeceklerini öğrenmelerine yardımcı olur. Bu tür saldırıları anlamak, çalışanların güvenli bir şekilde veri ve bilgi paylaşmasını engellemek için kritik bir beceridir. Eğitimler, çalışanların bilinçli ve dikkatli bir şekilde hareket etmelerini sağlar ve kuruluşun siber güvenliğini artırır. Bu sayede, sosyal mühendislik saldırılarına karşı daha savunmasız hale gelme riski azaltılır.

17 **Çevrimiçi tehditleri takip edin:** Çevrimiçi tehditleri takip etmek önemlidir çünkü güncel tehditler hakkında bilgi sahibi olmak, siber güvenliğinizi güncel tehditlere karşı korumanıza yardımcı olur. Siber güvenlik kaynaklarını düzenli olarak takip etmek, yeni tehditleri ve saldırı yöntemlerini öğrenmenizi sağlar. Bu bilgileri kullanarak koruma önlemlerinizi güncelleyebilir, zayıf noktaları belirleyebilir ve saldırılara karşı daha dirençli olabilirsiniz. Siber güvenlik kaynakları, sektörel yayınlar, siber güvenlik blogları, güvenlik şirketleri ve siber güvenlik toplulukları gibi çeşitli kaynaklardan elde edilebilir. Bu kaynaklar, sizi güncel tehditlerden haberdar eder ve güvenlik stratejilerinizi güncel tutmanızı sağlar.

18 **Acil durum tepki planı oluşturun:** Siber saldırı veya veri ihlali gibi acil durumlarla karşılaşmanız durumunda, hızlı ve etkili bir tepki verebilmek için bir acil durum tepki planı oluşturmanız önemlidir. Bu plan, ekiplerinizi belirli roller ve sorumluluklarla donatır ve gerektiğinde koordineli bir şekilde hareket etmelerini sağlar. Planınızda saldırı tespiti, olay yanıtı, iletişim yönergeleri ve etkilenen sistemlerin kurtarılması gibi adımları kapsayan bir süreç belirleyin. Ayrıca, planınızı düzenli olarak gözden geçirip güncelleyerek, değişen tehditlere ve şirketinizin ihtiyaçlarına uygun bir şekilde ayarlayın. Acil durum tepki planınız, kriz anında çalışanlarınızın etkili bir şekilde tepki verebilmesini sağlayarak şirketinizin siber güvenliğini güçlendirir ve zararları en aza indirir.





19 **İşbirliği yapın:** İşbirliği yapmak, şirketlerin aynı sektörde faaliyet gösteren diğer şirketlerle güvenlik konularında bilgi paylaşımında bulunmasını ve ortak güvenlik projelerine katılmasını ifade eder. Bu işbirliği, sektördeki güvenlik tehditleri ve en iyi uygulamalar hakkında bilgi alışverişini sağlar. Şirketler, birbirlerinin deneyimlerinden öğrenir, güncel tehditlere karşı daha iyi hazırlanır ve ortak güvenlik projeleri aracılığıyla kolektif güvenlik önlemleri geliştirir. Bu sayede şirketler birlikte çalışarak güçlü bir siber güvenlik ağı oluştururlar, sektörel siber saldırılara karşı daha dayanıklı hale gelirler ve genel olarak dijital ortamda daha güvenli bir iş ortamı oluştururlar.



20 Sürekli güvenlik iyileştirmesi yapın: Sürekli güvenlik iyileştirmesi yapmak, şirketlerin güvenlik önlemlerini düzenli olarak gözden geçirmesini ve güncel tehditlere karşı güncellemeler yapmasını içerir. Bu süreç, siber güvenlik açıklarını tespit etmek, riskleri değerlendirmek ve yeni savunma mekanizmalarını uygulamak için sürekli bir çabayı gerektirir. Şirketlerin saldırganların kullanabileceği yeni saldırı yöntemlerine ve zayıflıklara karşı bilgi sahibi olmaları ve bu bilgileri kullanarak güvenlik sistemlerini güncellemeleri önemlidir. Sürekli güvenlik iyileştirmesi, şirketlerin güvenlik önlemlerini en üst düzeyde tutarak siber saldırılara karşı daha dirençli hale gelmelerini sağlar ve veri güvenliğini sağlama amacıyla sürekli bir süreç olarak devam etmelidir.

Bu alınacak önlemler listesi genel bir rehber niteliğindedir ve her kuruluşun spesifik ihtiyaçlarına ve sektörel gereksinimlerine göre değişiklik gösterebilir. Şirketlerin bir siber güvenlik uzmanıyla çalışması ve özelleştirilmiş bir siber güvenlik stratejisi oluşturması gerekmektedir.