COVID-19 Siber Güvenlik

Güvenliği düşünerek normale dönmek

Devlet kurumları COVID-19 ile ilgili kısıtlamaları kademe kademe kaldırırken, çalışanlar da aşama aşama ofislerine dönüş yapmaya başlayacaklar. Sağlık ve güvenlik önceliklerini dikkate alarak, kuruluşların çalışma düzenlerinde gizlilik ve güvenlikle ilgili ne gibi önlemleri almaları gerekiyor?

Birinci öncelik – sağlık ve güvenlik

CISO'lar insan kaynakları, idari işler, hukuk ve BT ekipleri arasında geri dönüşle ilgili gerçekleştirilen konuşmalara dahil olmalı ve güvenlik ve gizliliğe vurgu yapılmasını temin etmeli. Risklerle ilgili bilgi sağlamanın yanı sıra, CISO'lar alınacak önlemlerle ilgili somut rehberlik de sağlamalı.

Bu konuşmaları desteklemek amacıyla aşağıdaki türden sorular kullanılabilir:

— Geçiş döneminde güvenlik ekibinin operasyonları nasıl olmalı, uzun vadede hangi süreçler ve yaklaşımlar korunmalı?

— Geçiş döneminde iş operasyonlarının güvenli bir şekilde devam ettirilmesi nasıl sağlanabilir? Bu dönemde geçici olarak kabul edilmesi gereken riskler nelerdir?

— Uzun vadede sosyal mesafeyle ilgili önlemler rahatlatıldıkça, fiziksel güvenlik ve veri korumasıyla ilgili düşünülmesi gereken önlemler neler olmalıdır?

Ekibiniz için yeni çalışma düzeni

Güvenlik ekipleri son birkaç aydır uzaktan çalışıyor, bu durum onları etkiledi mi?

— Kuruluşlar işe geri dönüyor, ancak okullar henüz dönmeyebilir — ekip içerisinde evde bırakamayacakları çocukları olanlar var mıdır? Ekibinizdeki kişilere bağlı olanlar için bakım ihtiyacı var mıdır?

— Risk altında veya takipte olan ve izolasyona devam etmesi gereken veya izolasyona girmesi gereken takım üyeleri var mı? Bunlarla ilgili çalışma yöntemi nasıl olmalı?

— Uzaktan çalışma döneminde ekip tarafından edinilen yeni uygulamalar ve alışkanlıklar oldu mu? Bunlardan ofise dönüş döneminde devam etmesi gereken hususlar nelerdir? Ekip olarak hangi alanlarda verimli veya verimsiz çalışmalar gösterdiniz?

Sosyal mesafeli bir güvenlik ekibi

Güvenlik ekipleri uzaktan çalışmaya alışmış olabilir, peki bu durumda ofise dönüşleri nasıl olacak?

— Ofiste hep birlikte ve eski cihazlarına erişebilecek şekilde aynı düzeni koruyarak oturmaları gerekecek mi, yoksa bu yeni döneme uyum sağlamak için farklı bir oturma ve cihaz düzenlemesi yapılacak mı?

— Ekibin tamamı aynı anda ofiste olacak mı? Diğer durumda güvenlik aktivitelerinde bir aksama söz konusu olabilir mi?

— Sunuculara, yedekleme sistemlerine ve güvenlik operasyon alanlarına erişimleri mümkün olacak mı? Kapalı ortamlarda kaç kişinin birlikte çalışabileceğine dair sınırlama olacak mı?

— Uzaktan çalışma esnasında ekipten ayrılanlar veya ekibe katılanlar oldu mu? Yeni giriş kartları veya donanım ihtiyacı var mı? Bunlar aynı şekilde sağlanmaya devam edilebiliyor mu?

— Ekiplerin ofise dönebilmeleri için gerekli sağlık kontrolleri ve testleriyle ilgili bir gereksinim mevcut mu, bunların gerçekleşmesi nasıl sağlanabilir?

Sosyal mesafe uygulamalarını destekleme

Güvenlik ekibinin yeni düzende çalışmasını sağlarken, iş birimlerinin de sosyal mesafeli çalışmalarda güvenlik ve gizlilikle ilgili hijyen kurallarına uymalarını sağlamak önemli bir öncelik.

— Çalışanlar ve tedarikçiler binada farklı alanlarda, toplantı odalarında veya kafeteryalarda mesafeli çalışıyor olabilirler; bu alanlar için fiziksel erişim kurallarının uygun olması temin edilebilir mi?

— Genel kullanım alanlarındaki ziyaretçilerle ilgili yenilenmiş rehberlere ihtiyaç olabilir. Bununla paralel, standart dışı çalışma alanlarında güvenliğe dikkat etmek için ekipleri bilgilendirmek gerekebilir.

— Sıkılaştırılmış donanımlar, kablo kullanımı ve korunaklı ekranlarla ilgili ilgili tedarik ve idari birimlerinizle irtibata geçmeniz gerekebilir.

— Fiziksel güvenlik önlemleri arasında enfeksiyon riskini artırabilecek kurallar mevcut olabilir mi? Parmak izi, manüel veya fiziksel güvenlik taramaları için alternatifleriniz mevcut mu? Fiziksel teması azaltmak için temassız doğrulama yöntemleri veya otomatik kapıların artırılması düşünülebilir mi?

Ofiste yeni yüzler

Bu dönemde yeni ekip arkadaşları katılmış olabilir. Bu durumda yetkisiz erişim teşebbüsleri nasıl tespit edilebilir?

— Sahadaki temizlik personeli ve tedarikçiler için erişim nasıl izlenebilir? Fiziksel erişimleri nasıl yönetiliyor? Erişimi kimlerin yaptığına yönelik ziyaretçi kartlarında bireysel takip mümkün mü?

— Pandemi sonrası derinleme temizleme faaliyetleri için, bu personelin normalde erişilmeyen alanlara erişmeleri gerekli olabilir (örn. sunucu ve iletişim odaları). Bu odalara erişimin kontrollü olduğunu nasıl gözetiyorsunuz? Bu girişler normal tüm girişler gibi kontrol ve gözetim altında tutuluyor mu?

— Çalışanların birçoğu halen serbest kıyafetle işe gelebilir veya maske giymek durumunda kalabilirler. Bu durumda yetkisiz erişimleri tespit etmek için ne gibi ek önlemler alınması gerekebilir?

İyi uygulamalara dönüş

Çalışanların ofise dönmesi aynı zamanda aylarca evde çalışıldıktan sonra güvenlikle ilgili iyi uygulamaların da tekrar devreye alınması anlamına gelecektir. Güvenlik ve gizlilikle ilgili hususlar bu doğrultuda tüm çalışanlara hatırlatılmalı:

— Giriş kartlarını taşımaya devam ediyorlar mı? Ekranlarını kitlediklerinden ve korunaklı tuttuklarından emin miyiz?

— Temiz masa kurallarıyla ilintili olarak, çalışanlar masa ve ofis cihazlarında gizli bilgi içeren evrak ve bilgilerin bulunmamasını sağlıyorlar mu?

— Temiz masa uygulamaları ve fiziksel güvenlik gözetimlerini yeniden gözden geçirmek gerekebilir. Bu dönemde işten ayrılan ve işe başlayanların olması buradaki riski bir miktar artıracaktır.

— Çalışanların evlerinde yer alan gizli belgeler olabilir mi? Bunları ofise getirmeleri ve uygun yöntemlerle gerekirse arşivlemeleri , elektronik ortama taşımaları veya uygunsa imha etmeleri gerekir.

— Uzaktan çalışmayla beraber taşınabilir cihazların kullanımı, basılı dokümanlar ve ek donanım kullanımları artmış olabilir, saha dışındaki bu kullanımın yeniden kısıtlanması gerekir.

Uzun vadeyi düşünebilmek

Kuruluşunuzun çalışma düzenlemeleri kalıcı olarak değişmiş olabilir.

— Ofise dönüş başlasa da, bazı çalışanların çok daha uzun vadelerde evden çalışmaya devam etmesi söz konusu olabilir. Bu durumda güvenlik, erişimler ve çalışanlardan kaynaklı olabilecek tehditleri yakından takip etmek ve izlemek gerekir.

— Evden çalışma birçok kuruluş için yeni ve kalıcı bir düzenleme olarak kalabilir, bu düzen için güvenlik kültürünü sürekli aşılamaları ve kuralları hatırlatmalıyız. Ofiste çalışmayanlar için poster ve TV ekranlarına alternatif ve yaratıcı bilgilendirme yöntemleri düşünülebilir.

— Güvenlikle ilgili geçirdiğiniz denetimler ve sahip olduğunuz sertifikasyon ve raporlarla ilgili yeni dönemdeki değişiklikler neler olacak. Hizmet kuruluşu güvence raporları, ISO27001, PCI-DSS vb standartlara göre denetim ve sertifikasyon hazırlıklarınızı yeniden gözden geçirmeniz gerekebilir.

İletişim

Servet Gözel
Direktör
Bilgi Teknolojileri Danışmanlığı
KPMG Türkiye
T: +90 530 940 50 95
E: servetgozel@kpmg.com

home.kpmg
home.kpmg/socialmedia