UZAKTAN ÇALIŞMA KILAVUZU

Her IT yöneticisi için Uzaktan Erişim Güvenliği denetim listesi

Toplumsal sorunlar oluştuğunda, evden çalışma seçeneği işletmeler için gereklidir. Ancak, çalışanları üretken ve işletmeyi çalışır durumda tutmak için uzaktan çalışma seçeneğine aceleyle geçmek kuruluşunuzu güvenlik açısından savunmasız bırakabilir. Siber suçlular hakkında bildiğimiz bir şey varsa o da fırsatlara atlamaktan çekinmedikleridir. İş gücünüzü konumuna bakılmaksızın korumaya yardımcı olmak için bu adım adım denetim listesini kullanın.

☐ Parola ilkelerini uygulama zamanı

Eğer burada rahat davrandıysan, şimdi ilkelerini güçlendirme zamanı. Uzun parolaları (veya daha iyisi cümleleri) zorunlu tutun, düzenli değişiklikleri zorlayın ve belirli sayıda başarısız girişten sonra hesapları kilitleyin. Çalışanlara, kişisel hesaplarını işte yeniden kullanamayacaklarını açıklayın.

☐ Çok faktörlü kimlik doğrulamayı kullanın

Ayrıca iki faktörlü kimlik doğrulama (2FA) olarak da bilinen bu yöntem çeşitli zorlama teknikleri kullanan veya derin webden kimlik bilgileri satın alan siber dolandırıcılara karşı kesinlikle en iyi savunma yöntemlerindendir. Bulut tabanlı hizmetler kullanıyorsanız ve MFA destekleniyorsa mutlaka kullanın. Kullanıcılarınızın sisteminize erişmesi gerekiyorsa araya mutlaka bir MFA çözümü koyun.

☐ Yerel ağınıza erişim için VPN kullanın

VPN, halka açık internetleri kullanarak şirkete bağlandığınız trafiği şifreler, böylece gelip giden veriler beklenmedik misafirler tarafından okunamaz. Ayrıca, VPN bağlantısı sayesinde yerel güvenlik ilkelerinizi uzaktaki cihazlara da uygulama şansı elde edersiniz. Zaten bazı çalışanlar için VPN kullanıyorsanız, yeni kullanıcıları kapsayacak kadar kapasiteye ve lisansa sahip olduğunuzdan emin olun. Çalışanlar dahili ağınızdaki kaynaklara erişiyorsa, VPN ve MFA'nın birleşimi şarttır.

☐ Mümkünse sanal masaüstü çözümü kullanın

Bu tür bir çözümle çalışanlar, bulutta veya veri merkezinizde bulunan sanal bir makineye uzaktan erişir. Tam olarak ofis tabanlı bir sisteme benzeyecek şekilde yapılandırılabilir. Avantajı hassas veri veya dosyaları sadece sanal makine de tutulur ve çalışanın ev bilgisayarlarına ve sistemlerine gönderilmez.

☐ Çalışanlara Wi-Fi konusunda dikkatli olmalarını hatırlatın

Tamamen kontrolünüzün dışında olan şey çalışanın kendi ev ağı ve ona bağlanan diğer cihazlardır. WPA2 güvenliğinin etkin olduğundan emin olmak için iş için kullanacağı sistemdeki tüm dosya paylaşımını kapatmalarını ve ev yönlendiricilerini veya Wi-Fi erişim noktalarını kontrol etmelerini söyleyin. Güvenlik anahtarı gerektirmeyen güvenli olmayan veya açık bir Wi-Fi erişim noktasına asla bağlanmamalarını hatırlatın.

Ev çalışanları için uç nokta güvenliğine yatırım yapın

Kişisel bir cihaz ile birlikte ücretsiz olarak verilen antivirüsün iş bilgisayarlarına yönelik çözümler kadar güvenilir olduğunu düşünmeyin. Tam özellikli bir kurumsal çözüm kişisel güvenlik duvarı, kötü amaçlı web sitelerine karşı koruma ve taşınabilir USB sürücülerdeki zararlı yazılımlara karşı koruma da dahil olmak üzere birden fazla savunma katmanıyla her türlü tehditlere karşı koruma sağlar. Buradaki en iyi seçenek, BT departmanınızın uzaktan yönetebileceği kurumsal bir uç nokta güvenlik paketidir.

Çalışanlar hassas dosyalara sahipse şifreleme gereklidir

Çalışanlar şirket dosyalarını kişisel cihazlarına indiriyorsa, onlara bir şifreleme (encryption) çözümü sağlayın. Kişisel dosyalarını şirket belgelerinden ayrı tutmaları ve şirket belgelerini şifreli bir klasöre kaydetmeleri konusunda ısrar edin. Ayrıca, açtıkları dokümanları kurumsal veri deposuna kaydettikleri bir ilke uygulayın, böylece uzaktan yedekleme konusunda endişelenmenize gerek kalmaz.

Oturum kapatma alışkanlığını yerleştirin

Çalışanlar mola verdiklerinde, bir veya iki dakikadan fazla bir süre cihazlarından uzakta oldukları için şirket ağından çıkış yapmalıdırlar. Bilgisayar evdeki diğer kişilerce de paylaşılıyorsa, bu bir zorunluluktur.

Düzeltme yamaları ve güncellemeleri gönderin

Tüm güvenlik önlemlerini güncel olduğundan emin olmak için, evden çalışanlarınıza sistemlerinde güncelleştirmeleri etkinleştirmelerini söyleyin. İç ortamınızın da güncel olup olmadığını, özellikle de 7/24 çalıştıkları için yamasız kalabilecek güvenlik açısından kritik öğeler çalışmadığını iki kez kontrol edin. Artık güncelleme almayan Windows 7 çalıştıran ev bilgisayarları konusunda ekstra dikkatli olun. Desteklenen bir sürüme yükseltilene kadar erişimi engellemeniz gerekebilir.

Çalışanlar için siber güvenlik eğitimi sağlayın

Ne kadar ileri teknoloji kullanırsanız kullanın, bir diğer önemli konu da çalışanlarınızın güvenlik konusundaki bilgisidir. Evden çalışanların kendilerine gelebilecek sahte kimlik doğrulama bildirimleri, patrondan gelebilecek ödeme onayları ve diğer kandırmacalar konusunda uyanık olmaları gerekiyor. Yeterli bilgiye sahip kullanıcılar bu tür kandırmacalara inanmazlar. Özellikle uzaktan çalıştıkları bu günlerde düzenli bilgilendirmeler ve eğitimler uyanık olmalarını sağlayacaktır.

Ve iyi haber...

Bulut tabanlı çalışma ortamları, sohbet ve konferans yoluyla çevrimiçi iş birliği ve diğer internet bağlantılı ve uzaktan erişim teknolojileri, çalışanların evlerinde de en az ofiste oldukları kadar üretken olmalarını sağlıyor. İşlerini eve götürürken, doğru güvenlik önlemlerini de götürdüklerinden emin olun.

ESET güvenlik çözümleri hakkında daha fazla bilgi için web sayfamızı ziyaret edin