

Evden Çalışma Sürecinde

Dikkat Edilmesi Gereken

Siber Güvenlik Hususları



Covid-19 milyonlarca insanın hayatını deęiřtirdi. An itibarıyla lkeler vatandaşlarına gerekmedike evden ıkmamaları ynnde aęrı yapıyor ve iř dnyasında da evden alıřma uygulamaları salgın nedeniyle gnden gne yaygınlařıyor. Daha nce evden alıřmaya dair bir altyapı hazırlamamıř birok řirket de uygulama iin acil altyapı hazırlayıp alıřanlarına evden alıřma talimatı vermek zorunda kalıyor.

İinde bulunduęumuz bu durumun, zellikle uzaktan alıřma deneyimine sahip olmayan kurumlar iin bu yeni alıřma ortamında oluřabilecek riskleri de gz nnde bulundurmak ve gerekli nlemleri almak nemli bir husus haline geliyor.

Sz konusu riskleri azaltmak iin evden alıřırken hem kurumunuzu hem de alıřanlarınızı korumak iin dikkat edilmesi gereken bazı temel siber gvenlik hususları ařaęıda listelenmiřtir.



1. Uzaktan alıřma politikalarının gzden geirilmesi

Kurumların uzaktan eriřim politikalarında hangi uzaktan eriřim yntemlerine izin verildięi, kimlerin uzaktan eriřim yetkisi olduęu ve uzaktan eriřim iin kullanılabilecek cihaz tipleri aıka belirtilmelidir. rneęin kuruma ait, kurum tarafından belirlenen gvenlik kriterlerine sahip bilgisayarlar kullanılarak birok kaynaęa eriřilebilirken alıřanların kendilerine ait bilgisayarlarından kritik olarak sınıflandırılmıř kaynaklara eriřimlere izin verilmemelidir.



2. Uzaktan erişim sistemlerinin güvenliğinin sağlanması

Evden çalışma döneminde kurumlar, çalışanlarının kurum varlıklarına erişimini sağlamak amacıyla uzaktan güvenli erişim sistemlerini daha sık kullanmaya başladılar. Uzaktan, güvenli erişim sağlayan sistemlerin kurum güvenlik politikalarını uygulayacak şekilde güvenli yapılandırıldığından emin olunması gerekir. Erişimin uçtan uca şifrelenerek sağlandığı bu yöntemde özellikle uzaktan erişim için kullanılan sistemlerin;

- En son güvenlik güncellemelerinin uygulanmış olduğu,
- Sistemin en iyi uygulama pratiklerine göre güvenli olarak yapılandırılmış olduğu,
- Kullanılacak kriptografik algoritmaların güncel olduğu,
- Olası bir arızada iş sürekliliğinin sağlanabilmesi için ilgili sistemlerin yedekli yapıda (high availability) yapılandırılmış olduğunun ve yedeklilik fonksiyonunun çalıştığının kontrolü,
- Konumlandırılmış olduğu ağ lokasyonundan kurum sistemlerine erişilirken, ağ trafiğinin güvenlik duvarı (FW), saldırı engelleme sistemi (IPS) gibi ağ güvenlik sistemlerinden geçirilecek şekilde konumlandırıldığı kontrolü,
- Servis engelleme/dağıtık servis engelleme (DoS/DDoS) saldırılarına karşı gerekli önlemlerin alındığının kontrolü sağlanmalıdır.

Uzaktan erişim sistemlerinin güvenliği özellikle önemlidir, çünkü çalışan makinelerinin şirket iç kaynaklarına erişmesi için bir yol sağlarlar. Ayrıca kurum tarafından verilen, üçüncü taraf kontrollü ve kullanıcı kişisel istemci aygıtları için güvenli, yalıtılmış bir uzaktan çalışma ortamı sağlarlar.

3. Uzaktan çalışma güvenlik riskleri

Uzaktan erişim üzerinden çalışan personelin ve kullandıkları cihazların karşı karşıya olduğu tehdit, kurum içinde barınan sistemler ve kurum içi çalışanlara kıyasla daha yüksektir. Bunun sebebi, personelin kurumun gözetimi altında olmayan birçok farklı ağdan ve birçok farklı fiziksel konumdan, kurum iç ağına erişim sağlıyor olmasıdır. Uzaktan çalışma güvenliği hakkında dikkat edilmesi gereken çeşitli risklerden bazıları aşağıda bahsedilmiştir.

3.1. Fiziksel güvenliğin yeterli olmaması

Kayıp ve çalıntı cihaz vakaları, kurum dışı çalışmalarda daha sık meydana gelmektedir. Bu tür durumlarda kurum için kritik ve/veya gizli bilginin başkaları tarafından elde edilebildiği bilinmektedir. Kurum dışında bulunan cihazlar fiziksel saldırılara ve kazalara karşı daha büyük bir risk altındadır.

3.2. Güvenliği sağlanmamış ağlar

Uzaktan erişim sağlayan personel, güvenliği sağlanmamış, güvenlik cihazlarının mevcut olmadığı ağlar üzerinden erişim sağlayabilir. Bu türlü ağlar üzerinde ortadaki adam (Man-in-the-Middle) saldırılarının riski çok daha büyük olmakla beraber toplam personelin bağlandığı güvensiz ağ sayısı haylice fazla olabilir. Bu durum ağ üzerinden gerçekleşebilecek saldırıların riskini büyük ölçüde artırmaktadır.



3.3. İç ağ için tasarlanmış sistemlere dışarıdan erişim sağlanması

Uzaktan çalışma süreci boyunca normal şartlar altında internet üzerinden erişime kapalı hassas sunucu ve uygulamaların dışarıdan erişilebilir hale gelmesi gerekli olabilir. Bu durum, nispeten güvensiz ve/veya hassas veri barındıran sistemlerin karşı karşıya olduğu riski büyük ölçüde artırmaktadır.

4. Uzaktan çalışma yol haritası oluşturmak

Uzaktan çalışma için kurumsal seviyede bir yol haritasının oluşturulması ve takip edilmesi gerekmektedir. Bunun için izlenebilecek adımlar aşağıda belirtilmiştir.

4.1. Ağa bağlanacak cihazların belirlenmesi

Ağa uzaktan bağlanacak cihazların tamamının listesi uzaktan çalışma süreci başlamadan önce çıkartılmalı, gerekli beyaz liste (whitelist) ve erişim kontrol listeleri uzaktan çalışma süreci başlamadan önce oluşturulmalıdır.

4.2. Uzaktan çalışacak kullanıcıların belirlenmesi

Uzaktan çalışacak personelin uzaktan çalışma sürecinin öncesinde bir listesinin çıkartılması gerekmektedir. Bu listeden yola çıkarak hangi kullanıcıların nereye erişmesi gerektiği ve hangi yetkilere ihtiyacı oldukları doğrultusunda katmanlı bir yetki şeması oluşturulmalıdır.



4.3. Ağa bağlanan cihazların güncel tutulması

Kurum içinde çalışmayan personel, kurumun kontrolünde olmayan birçok farklı ağ üzerinden (Yönlendirici, Bilgisayar, Telefon, Access Point vb.) erişim sağlayacaktır ve bu durumda kullanılan istemci cihazlar birçok farklı tehdide açık olacaktır. Bu tür tehditlere karşı ilgili sistemlerde güvenlik yamalarının yapıldığından ve kullanılan hizmet ve işletim sistemlerinin güncel olduğundan emin olmak elzemdir.

4.4. Ağa bağlanan cihazların güvenliği

Ağa bağlanan tüm cihazların, ister uzaktan ister yerel ağdan bağlanıyor olsun, kurumun belirlediği güvenlik kriterlerine uyum sağlıyor olması gereklidir. İstemciler kurumun güvenlik politikalarına uygun olarak yapılandırılmış, güvenlik yamaları uygulanmış, yerel yönetici yetkisine sahip olmayan güncel bir işletim sistemine sahip olmalıdır. Zararlı yazılımlardan korunabilme amacı ile de güncel imzalara sahip son kullanıcı güvenlik yazılımlarının (Antivirus, IPS , EDR vb.) aktif olarak çalışmasının sağlanması gerekmektedir.



4.5. Uzaktan çalışma süresi boyunca iletişim

Çalışanlara bu süreç içerisinde uygulanacak olan politikaların, kullanılacak yetkilendirme mekanizmalarının, bulut çözümlerinin nasıl kullanılacağı ve uzaktan erişim araç ve yöntemlerinin tamamının çalışanlara şeffaflık içerisinde bildirilmesi önemlidir. Böylelikle bu yeni durumda herkesin değişime hızlı bir şekilde uyum sağlaması mümkün olacaktır.

4.6. Kullanılan altyapı kapasite kontrolü

Uzaktan çalışma modelini hali hazırda benimsememiş şirketlerde yaşanabilecek altyapı kapasite (lisans, donanım) sorunları hızlıca tespit edilmeli ve buna uygun kapasite yükseltme işlemleri yapılmalıdır. Kullanılan kurumsal altyapıdaki sistemlerin uzaktan çalışacak personel ve kullanılacak cihaz sayısı için yeterli olduğunun kontrol edilmesi hizmetin devamlılığının sağlanması açısından oldukça önemlidir.

4.7. Veri şifreleme

Yukarıda da belirtildiği üzere hırsızlık ve kaybolma gibi olaylar uzaktan çalışma dönemlerinde artış gösterebilir. Veri gizliliğini sağlayabilme adına cihazlar üzerindeki kritik verilerin şifreli tutulması, mümkünse tüm diskin şifrelenerek kullanılması önerilmektedir.



4.8. Ayırık tünelleme (split tunneling) kullanımı

Ayırık tünelleme (Split tunneling), bazı programlar sanal özel ağ (VPN) kullanırken, geri kalan diğer programların varsayılan internet bağlantısı üzerinden direkt olarak erişim sağlanmasıdır. Bu durumda kullanıcı işlemlerinin bir kısmı kayıt ve kontrol altında tutulurken, bir kısmı tamamen güvenlik birimlerinin göremeyeceği bir şekilde gerçekleşir. Ayırık tünelleme kullanılırken hangi trafiğin tünel üzerinden, hangi trafiğin kullanıcı bireysel internet bağlantı üzerinden akacağı net bir şekilde belirlenmelidir.

5. Kimlik ve erişim yönetimi

5.1. Çok Faktörlü Kimlik Doğrulama (Multi Factor Authentication - MFA) kullanımı

Kullanıcı adları ve parolalar çalınabilir, sızdırılabilir veya kaba kuvvet (bruteforce) ve oltalama (phishing) gibi saldırılar ile elde edilebilir. İnternete açık olan sistemler için tehdit unsuru oluşturan saldırılara karşı koyabilmek adına MFA erişim yöntemlerini kullanmak riski büyük ölçüde azaltacaktır. MFA, erişim isteyen kullanıcının aslında iddia ettiği kişi olduğu konusunda güveni artırmaya yardımcı olmak adına eklenen ayrı bir güvenlik katmanıdır. En sık kullanılan MFA yöntemlerinden biri, telefona SMS göndermektir.

5.2. Güvenli cihaz (Device Trust) kullanımı

Ağa bağlanabilecek cihazlar önceden listelenerek, bu cihazlar dışındaki herhangi bir cihazın ağa bağlanmasının engellenmesi gerekmektedir. Böylece herhangi bir şekilde uzaktan erişim için gerekli bilgileri elde eden saldırgan, ağa kendi cihazını bağlayamayacaktır.

Ağa bağlanan cihazın güvenilir olduğunu kontrol etmek için ilgili cihaza bir sertifika tanımlanması yöntemi kullanılabilir. Bu sertifikanın güvenliği kurum için kritik önem taşır. Cihazı ele geçiren bir saldırgan, sertifikayı dışarı aktarıp başka bir bilgisayarı güvenli olarak tanıtamamalıdır.

Yönetilemeyen cihazlar varsayılan olarak veri ve kaynaklara kısıtlı erişime sahip olmalıdır. Bu sınırlandırmaların doğru bir şekilde çalışıyor olduğundan emin olmak kritik önem taşımaktadır.

5.3. Yetkili kullanıcılar için ayrı güvenlik katmanları kullanılması

Sistemdeki yüksek yetki sahibi, ayrıcalıklı kullanıcıların da uzaktan çalışma senaryolarına göre uyumlu bir şekilde sistemlere erişmesi sağlanmalıdır. Burada gerekli katmanlı yapı oluşturulmalı, buna göre yetkilendirme ve izleme yürütülmelidir.

6. Gölge BT (Shadow IT) tehdidi

Kurumsal bilgi teknolojileri departmanının onayı ve desteği olmadan geliştirilip kullanılan teknoloji çözümleridir. Bunlara örnek olarak; bulut (cloud) uygulamaları, kişisel cihazlar, excel makroları ve benzeri araçlar verilebilir. Bu teknolojilerin kurumun kendisi, kurumun verileri ve kullanıcı için ayrı bir zafiyet oluşturup oluşturmadığı kontrol edilmelidir.

Çalışanlara uygun, kurumsal bulut çözüm alternatifleri sunmak ve uzaktan çalışma süreci öncesinde kullanılacak çözümlerin detaylı bir şekilde planlanması gerekmektedir. Böylelikle kullanıcılar kurumun kontrolü dışında olan uygulamaları kullanmaktansa, kurum tarafından sunulan ve kontrol edilen çözümleri kullanmayı tercih edeceklerdir. Kullanıcılar, başka çözümler kullanmamaları adına bilinçlendirilmeli ve olası Gölge BT (Shadow IT) vakaları tespit ve takip edilmelidir.

7. Kullanıcı farkındalığı

Alınan önlemler ile kurumun ancak en zayıf halkası kadar güçlü olabileceği kabul edilmelidir. Güvenlik alanlarında ne kadar önlem alınırsa alınsın, en zayıf halkanın hemen hemen her zaman son kullanıcı olduğu değerlendirilmektedir. Bu sebeple teknik önlemlerin yanında son kullanıcı için farkındalık yaratmak, alınabilecek en kritik tedbirler arasındadır.

Kullanıcıların farkındalığını arttırma ve olası tehditlere karşı hazırlıklı olunmasını sağlama amacı ile evden çalışma esnasında karşılaşılabilecek riskler, uyulması gereken önlemler ve bir tehdit ile karşılaşıldığında bildirim yapılması gereken birimin iletişim bilgileri hakkında sıklıkla bilgilendirmeler yapılmalıdır.

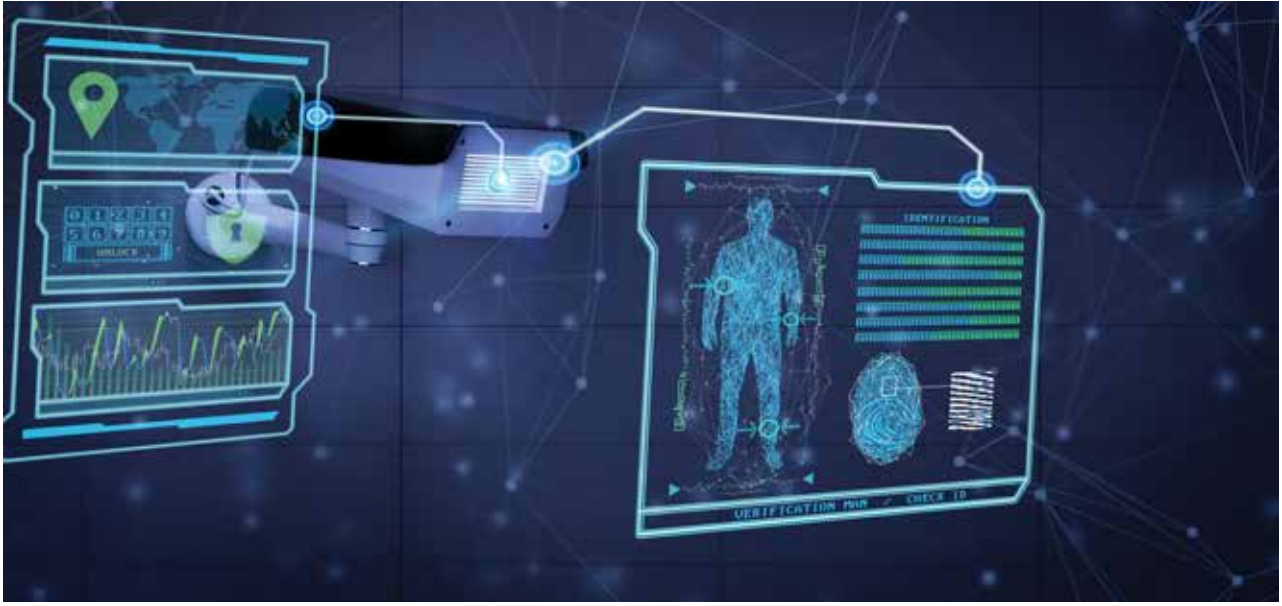
8. Düzenli güvenlik testleri

Evden çalışma süresi boyunca, gerçekleştirilen güvenlik testleri normal şartlar altında olduğu gibi devam etmelidir. Bu gibi zor zamanlarda güvenlikten sorumlu personel kurumun farklı ihtiyaçlarına odaklandığından rutin yapılması gereken zafiyet yönetimi gibi işlerinin aksaklığa uğradığı saldırganlar tarafından bilinmekte ve durum istismar edilebilmektedir. Bu gibi durumlarda var olan güvenlik seviyesini korumak da kritik hususlardan biridir.



9. İzlenebilirlik

Ağda gerçekleşen olayları izleme, araştırma ve beklenmedik olaylar sonrası olay araştırması yürütülebilecek bir şekilde log tutulmalıdır. Özellikle evden çalışmanın kullanıldığı bu dönemde, uzaktan bağlantı gerçekleştirilen tüm sistemlere ait logların detaylı olarak tutulması ve merkezi log kayıt yönetimi sistemine (SIEM) gönderilmesi ve alarmların takibi gerekmektedir. Bu sayede olası bir ihlal sırasında neler olduğunu anlamak kolaylaşacak ve olay müdahale süreçleri iyileştirilmiş olacaktır.



10. Video konferans gizliliğine dair önlemler

Evden çalışma süresi boyunca personelin video konferans uygulamaları kullanımında büyük bir artış normal olacağından, video konferans yaparken dışarı verilen veri ve kullanılan uygulamaların sağladığı gizlilik üzerinde durmak önemli hususlardan biridir.

Toplantı ve benzeri ihtiyaçları gidermek için gerçekleştirilecek video konferansların başkaları tarafından erişilebilir olmayacağının kontrol edilmesi gerekmektedir. Buna ek olarak, uçtan uca şifreleme kullanan bir program kullanılmalıdır. Kullanılan programın, son kullanıcılardan ne tür bilgiler topladığı detaylı bir şekilde incelenmelidir. Bu hususa dikkat edilmezse, kuruma ve kurum tarafından kullanılan sistemlere dair veri ihlali gerçekleşmesi mümkündür.

Gizli projelerde, bu tür çözümlerin kullanılması tavsiye edilmemekle birlikte, yapılan konuşmalar sırasında gizli bilgi paylaşılmaması konusunda kullanıcıların bilinçlendirilmesi tavsiye edilmektedir. Bu tür çözümlerin kullanımında, bulut sağlayıcılardan ziyade, kurumun kontrolü altında olacak şekilde sağlanan, yerinde (on-premise) çözümler tercih edilmelidir.

Bu noktada herhangi bir gizlilik derecesi taşıyan proje ve çalışmalar için, yurt dışı menşeli çözümlerin yerine yerel çözümlerin tercih edilmesi tavsiye edilir. Saldırganların bu tür durumlardan faydalanarak sık kullanılan programların içine zararlı yazılım yerleştirdikleri ve bu programları anımsatacak sahte programlar geliştirdikleri bilinmektedir. Bu nedenle bu tür programları indirirken, doğru kaynaktan indirilmesi konusunda personel bilgilendirilmeli ve sağlanandan farklı alan adlarından gelen programların kullanılmaması gerekmektedir.

11. Sonuç

Evden çalışmaya geçiş bazı kurum ve kuruluşlar için çeşitli zorluklar oluştursa da, an itibarıyla çoğu kurum için bir ihtiyaç olarak değerlendirilmektedir. Çeşitli durumlarda performans artışı sağlamakla birlikte, bunun yanında güvenlik riskleri de getirmektedir. Bu güvenlik risklerini yönetebilmek için, uzaktan çalışmaya geçiş öncesi bir hazırlık gerçekleştirilmesi ve uzaktan çalışma süreci boyunca normal şartlar altında düzenli olarak gerçekleşen kontrollerin aksatılmaması gerekmektedir. STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. Siber Füzyon Merkezi tarafından sunulan tavsiye ve önerilere uymak, uzaktan çalışmanın getirdiği riskleri büyük ölçüde azaltacak, uzaktan çalışmaya uyum sağlama süresinde güvenlik adına alınan eylemleri kolaylaştıracaktır.