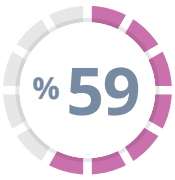
bugbounter

Tedarik zincirinin siber güvenliği

Haziran 2020

www.bugbounter.com

Kurumlar ve tedarik sağlayan iş ortakları, her geçen gün birbiriyle daha bağlantılı hale geliyor ve dolayısıyla siber güvenlik tehditleri tedarik zincirinde yer alan iş ortakları üzerinden anlaşmalı şirketleri derinden etkiliyor. Her ne kadar şirketler en gelişmiş güvenlik yöntemleriyle kendilerini koruma altına alsa bile tedarikçilerin ve iş ortaklarının da benzer seviyede güvenliğe sahip olduğundan emin olmaları çok önemli. Bu yüzden şirketlerin bünyelerindeki hassas verileri etkin bir şekilde koruyabilmesi için tedarik zinciri üzerinden karşılaşabileceği siber saldırı potansiyelini öncelikle dikkate alması gerekiyor.



Ponemon Institute'un gerçekleştirdiği Data Risk in the Third-Party Ecosystem isimli araştırmaya göre şirketlerin yüzde 59'u, siber saldırıya maruz kalan sistemlerine dahil olan tedarikçileri üzerinden etkileniyor.

Öte yandan yine aynı araştırmaya göre bu iş ortakları üzerinden oluşabilecek riskleri başarılı bir şekilde ortadan kaldırdığını belirten şirketler ise sadece yüzde 16'lık bir kısmı oluşturuyor.

Cevaplayanların yüzde 22'si de birlikte çalıştığı tedarikçinin geçmiş 12 ay içerisinde bir veri ihlali yaşayıp yaşamadığını bilmediğini belirtiyor.

Tedarik zinciri saldırısı, bir iş ortağı veya tedarikçi gibi anlaşmalı bir şirket üzerinden sızması anlamına geliyor. Bu tanım üzerinden yola çıkıldığında diğer paydaşları kontrol etmek başlangıçta biraz zahmetli görünse de bunu yapmanın ve şirketi eksiksiz bir şekilde korumanın yolları var.

Peki bu yollar neler?

Herhangi bir iş ilişkisine başlamadan önce sağlayıcıları test etmek ilk sırada geliyor.

Bu noktada şirketler, tedarikçilerinden güvenlik testleri yaptırmalarını isteyebilir. Farklı denetimler ile "Hangi güvenlik araçlarını kullanıyorlar?" "Hangi erişim ilkesini tercih ediyorlar?" "Yamalarını en kısa zamanda güncelliyorlar mı?" gibi soruların cevaplarına ulaşabilirler. Ayrıca şirketler, sızma testleri gibi yöntemlerle sağlayıcıyı kendisi de güvendiği bir iş ortağına test ettirebilir. Ek olarak tedarikçilerinin siber saldırılara karşı sigorta yaptırmalarını da isteyebilir.

Tüm bunları göz önünde bulundurduğumuzda aslında tedarikçilerin hizmet verdikleri şirketlere karşı şeffaf olması, ne kadar güvenli olduklarını göstermesi ve geliştirici önerilere açık olması gerekiyor. Tedarikçilerle yapılacak sözleşmelerde güvenlik ve mahremiyet (gizlilik) ile ilgili maddelerin bulunması ve cezai şartlarla bu maddeleri güçlü hale getirmek elbette önemli. Ancak sözleşmelerin, tek başına ana şirketleri yeterince koru(ya)madığı bir çok geçmiş olayda kanıtlandı.

Bu aşamada tedarikçiye aşağıdaki sorular da sorulabilir:

- Yazılım ve donanım tasarımı belgelenmiş mi?
- Bilinen açıklar ürünün tasarımında bulunuyor mu?
- Sağlayıcı, yeni ortaya çıkan zafiyetlere nasıl karşılık veriyor?
- Olası bir sıfır-gün açığını nasıl giderebiliyor?
- Yapılandırma yönetim süreçlerinin performansı nasıl?
- Kötü amaçlı yazılım koruması ve tespit süreci hangi seviyede?
- Güvenlikle ilgili hangi koruyucu önlemler var?
- Hem siber hem de fiziksel hangi erişim kontrolleri kullanılıyor? Bunlar nasıl belgeleniyor ve test ediliyor?
- Hangi tür çalışanlara özgeçmiş kontrolü yapılıyor? Bunlar nasıl belgeleniyor ve test ediliyor?

- Dağıtım süreci ne kadar güvenli?
- Onaylanmış ve yetkilendirilmiş dağıtım kanalları açık bir şekilde belgeleniyor mu?
- Ürünün yaşam döngüsünde güvenlik nasıl sağlanıyor?

İkinci seçenek ise veri erişimini devamlı gözlemlemek.

Bunun için ilk adım hem şirket içinde hem de tedarikçi tarafında kimin hangi verilere erişebildiğini net bir şekilde belirlemek. Şirketler böylece paydaşlarıyla ne ölçüde bağlantıda olduğunu ve hangi sistemleri kimin erişimine açtığını görebilir.

Üçüncü olarak şirketler tedarikçilerinin kritik çalışanlarını eğitebilir ve paydaşlarının kendilerini geliştirdiğinden emin olabilir.

Çünkü siber güvenlik eğitimleri, farkındalık yaratmak için büyük role sahip. Günlük işlemlerde birçok farklı teknoloji sıklıkla kullanılıyor ve bunun sonucunda ortaya karmaşık bir yapı çıktığı için yeni riskleri tespit etmek neredeyse imkânsız hale gelebiliyor. İnsan hatasından oluşabilecek riskler de en az teknoloji kadar önemli. Tedarik zincirleri daha fazla paydaşın dahil olmasıyla daha karmaşık hale geliyor ve gerekli teknolojileri kullanan insan sayısı artıyor ancak bilgi ve beceriler aynı hızda artmıyor.

Şirketlerin tedarikçileri için organize edeceği bir eğitimde; sık karşılaşılan parola hatalarına, oltalama (phishing) denemelerini tespit etmeye, iş e-postasının ele geçirilmesine (Business E-mail Compromise, BEC) ve tedarikçi e-postasının ele geçirilmesine (Vendor E-mail Compromise, VEC) mutlaka değinmesi gerekiyor. Bunlara ek olarak kötü amaçlı yazılımların türlerini belirlemeyi öğretmesi, şirket içinde yaşanabilecek şüpheli durumlara karşı dikkati artırması ve bu durumlarla karşılaşıldığında nasıl davranılması gerektiğine dair bilgiler paylaşması da kritik.

Şirketin çok katmanlı bir koruma yazılımıyla korunması gerekiyor.

Her ne kadar son kullanıcıların ellerindeki cihazları ve şirket ağlarını korumak önemli olsa da iyi bir yama yönetimi, yönetici erişiminin iyi bir şekilde organize edilmesi gibi detaylar da bir saldırının gerçekleşmesini belirleyen faktörler arasında yer alıyor. Dolayısıyla tedarikçi bünyesindeki BT ekiplerinin verimli bir şekilde kullanabileceği yazılımların tercih edildiğinden emin olmak gerekiyor.

Yakın zamanda tedarik zincirinin siber güvenliğine yönelik birçok saldırı gerçekleşti.

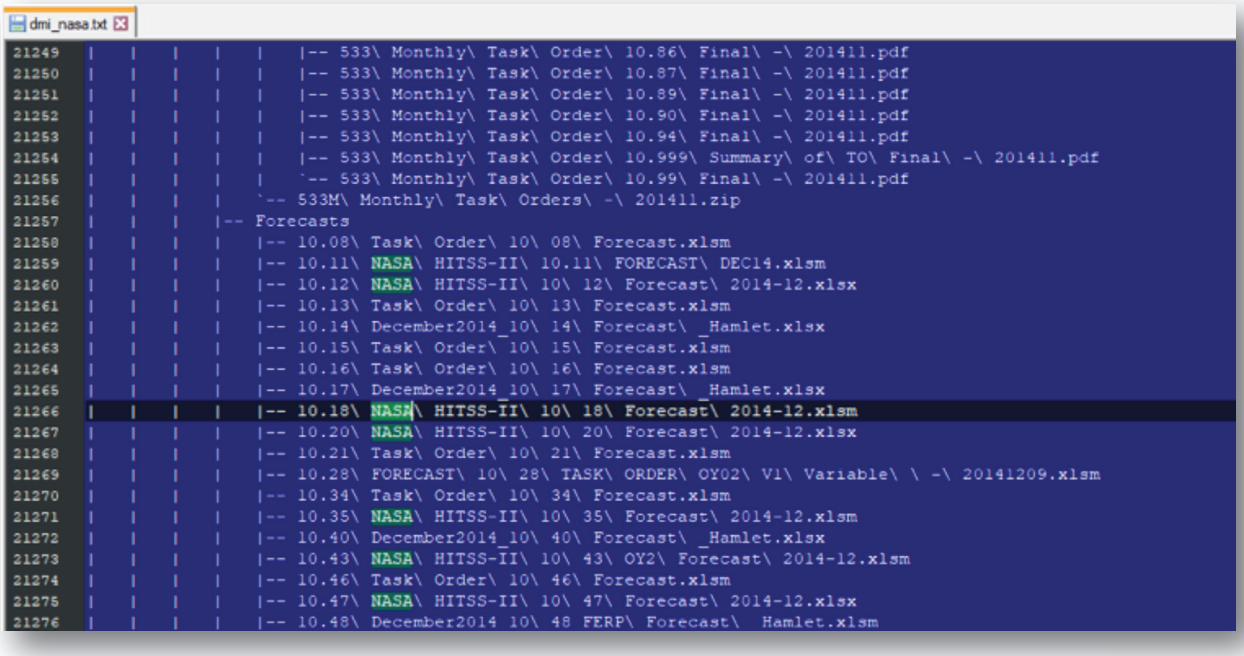
Amerika'nın en büyük zincir mağazalarından olan **Target'in yaşadığı veri ihlali**, tedarikçilerinden birinin zafiyeti üzerinden gerçekleşti. Bir soğutma sistemi satıcısı, oltalama e-postasını açıyor ve bankacılık trojanı Zeus'un bir türü olan Citadel şirket bünyesinde kullanılan bir cihaza yükleniyor. Devamında ise saldırganlar şirket çalışanlarının giriş bilgilerini ele geçirdi. O dönemde gerçek zamanlı bir koruma sunan ve bu saldırının önüne geçebilecek kötü amaçlı yazılımlara karşı bir program bulunmuyordu.

Devamında ise saldırganlar hangi noktadan giriş yapacağını keşfedip Target'in iç ağına sızıyor. Target'in sunucularını ele geçiren saldırganlar, POS sistemlerine de erişebiliyor. Bu saldırının ardından Target güvenliğini iyileştirmeye odaklandı. Bu kapsamda görüntüleme ve kayıt süreçlerini iyileştirdi, iş ortaklarının erişimini gözden geçirdi, gerekli yerlerde kısıtladı, belirli tedarikçilerin yetkilerini azalttı ve çalışanlarını daha güvenli şifreler kullanmaları için eğitti.

Büyük şirketlerin, politikacıların ve ünlülerin vergi kaçırma işlemlerine dair 13 milyondan fazla belgeden oluşan Paradise Belgeleri, Appleby hukuk firmasına yapılan saldırı üzerinden ele geçirilerek sızdırıldı. Belgeleri sızdırılan 120.000'den fazla kişi ve şirketin arasında Prens Charles ve Kraliçe II.Elizabeth, Kolombiya Başkanı Juan Manuel Santos ve ABD Ticaret Bakanı Wilbur Ross gibi önemli kişiler de yer alıyor.

Bu hafta yayınlanan bir blog yazısında DopplePaymer fidye yazılımı çetesi, BT ve siber güvenlik hizmetleri sağlayan Maryland merkezli Digital Management Inc. (DMI) şirketinin ağına başarıyla sızdığını söyledi.

DMI'nin müşteri listesinde Fortune 100 listesinde yer alan birkaç şirket ve aralarında NASA'nın da olduğu birçok devlet kurumu var. NASA ile ilgili dosyalara eriştikleri ve DMI'nin NASA ile ilgili altyapısını ihlal ettiklerini açıkça gösteriyor.



DopplePaymer, iddialarını desteklemek için grubun çalıştığı bir dark web portalına 20 arşiv dosyası gönderdi.

IBM'in açıkladığı rakamlara göre kritik bir veri ihlali ortalama 3,9 milyon dolarlık mali zarara ve itibar kayıplarına neden oluyor.

Profesyonelce yönetilen kitle kaynağı üzerinden uygun maliyetlerle çok daha hızlı ve kapsamlı bir şekilde alınabilecek sızma testi hizmetleri ve buna bağlı önlem paketleri, ihlallerden kaynaklı astronomik maliyetlerin daha da artmasını engelleyecek güç olacaktır.

Kaynaklar:

- https://heimdalsecurity.com/blog/supply-chain-cyber-security/
- https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf
- https://medium.com/@KodiakRating/the-cyber-security-of-supply-chains-whos-the-real-risk-man-or-machine-ecdcc365d49d
- https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf
- https://databreachcalculator.mybluemix.net/?_ga=2.96830426.436800262.1577141175-921129177.1577141175&cm_mc_uid=18423071444915771411736&cm_mc_sid_50200000=91922601577141173609&cm_mc_sid_52640000=36284071577141173618