Teknoloji Uygulaması

Chubb, Artan Siber Riskleri Esnek ve Sürdürülebilir bir Yaklaşımla Ele Alıyor

Siber sigorta teminatı bölümü; Yaygın Olaylar, Fidye Yazılımı Olayları ve İhmal Edilen Yazılım Güvenlik Açıklarına yönelik risklerin ne ölçüde aktarılacağı ve ne ölçüde tutulacağı konusunda poliçe sahibine esneklik sağlar.

CHUBB®

Yaygın olaylar

Dünya her geçen yıl daha da dijital ve birbirine bağlı bir hâl almaktadır. Binlerce ya da milyonlarca şirket yaygın kullanılan yazılım programları, iletişim ve teknoloji platformlarından faydalanmakta ve genellikle bunlara güvenmektedir. Bu yaygın kullanılan platformlardan veya teknolojilerden birinde meydana gelebilecek tek bir saldırı ve/veya arıza sigorta sektörünün sigortalama kapasitesini aşan büyük bir risk oluşturabilir. Chubb, poliçe sahiplerine teminat netliği ve pazar istikrarı sağlamak için bu "Yaygın Olaylara" yönelik kesin ve belirli limitler, konservasyonlar ve koasürans sunar.

Teminat altına alınan Yaygın Olay riskleri şunlardır:

Yaygın Yazılım Tedarik Zinciri Güvenlik Açıkları
Bu saldırılar temelde kötü niyetli kişilerin güvenilir, sertifikalı yazılımlar aracılığıyla sistemlere girmesine izin veren bir Truva atından doğar.

Gerçek hayattan örnekler > Solorigate (2020), NotPetya (2017)

Yaygın ve Ciddi Sıfır Gün Güvenlik Açıkları
Bunlar, siber suçlular tarafından bilindiği halde henüz başkaları tarafından bilinmeyen, kolayca suistimal edilebilen, ciddi nitelikteki ve çoğu zaman koruma içermeyen bazı yazılım güvenlik açıklarından kaynaklanan saldırılardır.

Gerçek hayattan örnek > Hafnium (2021)

Yaygın ve Ciddi Nitelikteki Bilinen Güvenlik Açıkları
Bunlar, yama uygulanmamış ciddi ve bilinen yazılım güvenlik açıklarından kaynaklanan saldırılardır. Bu güvenlik açıkları, suistimal edilmelerinin kolay olması, sınırlı erişim öncelikleriyle uzaktan dağıtılabilmesi ve önemli olumsuz etkilere sebep olabilmeleri nedeniyle ciddi olarak kabul edilir.[1]

Gerçek hayattan örnek > MSSP Saldırısı (2021)

Diğer Tüm Yaygın Olaylar
Belirli türdeki siber saldırılar çok sayıda mağduru hedef alıp eş zamanlı veya otomatik olarak gerçekleştirilebilir ve sonuçta felaket niteliğinde bir siber olaya neden olabilir. İnternet ve bazı telekomünikasyon hizmetleri kritik toplumsal altyapı seviyesine yükselmiş olup; bazı büyük bulut bilişim firmaları o kadar yaygın olarak kullanılmaktadır ki, yaşanan bir kesinti binlerce işlemi ya da milyonlarca şirketi etkileyebilecektir.

Gerçek hayattan örnek > Virginia Bulut Kesintisi (2020)

1 NIST Security Vulnerability Trends in 2020: An Analysis (2021). https://www.redscan.com/media/Redscan_ NIST-Vulnerability-Analysis-2020_v1.0.pdf adresinden alınmıştır.

Yaygın Olay metni aşağıdaki hususların dahil olduğu net ve makul hasar tespiti kuralları içerir:

Olay müdahalesi masrafları için ancak bir olayın Yaygın Olay olduğu tespit edildikten sonra Yaygın Olay limitleri kullanılır ve bu tespitten önce maruz kalınan masraflar iade edilmez.

Poliçe sahipleri, karşılıklı olarak bir olayın Yaygın Olay olduğu kararlaştırıldığında incelemeyle ilgili bazı verileri paylaşmamayı tercih edebilir.

Poliçe sahiplerinin, kuruluşlarının ihtiyaçlarını en iyi şekilde karşılayan teminatı satın alabilmeleri için tüm siber olaylar şu şekilde sınıflandırılmıştır:

- Sınırlı Etkiye Sahip Olaylar (ör. "olağan iş" kaybı kurallarına tabi yerel bir olay) veya
- Yaygın Olaylar (ör. limit, konservasyon ve koasürans gibi yapısal hasar tespit farklılıkları içeren sistematik bir olay)

Fidye Yazılımı

Fidye yazılımı saldırıları hem sıklık hem de şiddet bakımından önemli bir artış göstermiştir. Poliçe sahiplerinin maruz kaldığı kaybın etkileri fidye miktarının değerinden çok daha büyüktür. Fidye ödense de ödenmese de poliçe sahipleri genellikle mahkeme masrafları, adli soruşturma masrafları, iş kesintisi kayıpları, dijital verileri kurtarma masrafları ve doğabilecek diğer mali sorumluluk ve yasal savunma masraflarına maruz kalır.

Fidye Yazılımı teminatı, Fidye Yazılımı sonucu maruz kalınan kayıplara yönelik teminat limitleri, konservasyon ve koasürans için özelleştirme sunar.

İhmal Edilen Yazılım Güvenlik Açıkları

Yazılımları güncel tutmak siber riskten iyi bir şekilde korunmak için önemli bir unsurdur. Siber suçluların güvenlik açığı olan yazılımlardan istifade etmesine fırsat vermeden bu yazılımların yamalanması birçok kaybın önüne geçebilir ancak bazı kuruluşlar yazılım yamalarında geç kalabilir. Bazen yazılım güncellemelerinin kullanıma sunulmadan önce test edilmesini gerektiren meşru nedenler vardır ve uyumluluk, kapasite veya basit lojistik sorunları, iyi yönetilen bir bilgi güvenliği kuruluşunun dahi yamaları kullanıma sunulduğu ilk gün veya hafta içinde uygulamasına engel olabilir. Bu nedenle Chubb, poliçe sahiplerine ABD merkezli *National Institute for Standards and Technology (NIST)* tarafından yürütülen Ulusal Güvenlik Açıkları Veri Tabanında, Yaygın Güvenlik Açıkları ve Riskler (CVE'ler) olarak yayınlanan yazılım güvenlik açıklarını yamalamak için 45 günlük bir ek süre sağlamaktadır.

Bu 45 günlük ek süre dolduktan sonra, poliçe sahibi ile sigortacı arasındaki İhmal Edilen Yazılım Kullanım riski paylaşımı giderek poliçe sahibine geçer ve poliçe sahibi, güvenlik açığının 46., 90., 180. ve 365. günde yamalanmaması halinde kademeli olarak daha fazla risk almış olur.

Daha fazla bilgi için

chubb.com/uk/cyber

Chubb. Insured.℠

Bu dokümanda yer alan içeriğin tamamı yalnızca genel bilgi verme amaçlıdır. Herhangi bir ürün veya hizmetle ilgili olarak herhangi bir kişi veya kuruluşa verilen özel bir tavsiye veya öneri niteliğinde değildir. Tüm teminat hükümleri ve koşulları için, düzenlenen poliçe belgelerini inceleyin. Chubb European Group SE Merkezi İngiltere Türkiye İstanbul Şubesi, Büyükdere Caddesi no 100-102, Maya Akar Center B Blok Kat:5, Esentepe 34394, Istanbul, Turkiye Şubesi olduğumuz Chubb European Group SE Fransız sigortacılık kanunu hükümlerine tabii olup, sicil numarası 450 327 374 RCS Nanterre ve kayıtlı adresi de La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, Fransa'dır. Chubb European Group SE'nin ödenmiş sermayesi 896,176,662 Euro'dur. Chubb European Group SE Türkiye'deki faaliyetlerini İstanbul'daki Şubesi aracılığı ile yapmakta olup, Türkiye Şubesi'nin kayıtlı adresi Büyükdere Caddesi, No:100-102 Maya Akar Center, Kat:5 Esentepe Şişli Istanbul'dur. Türkiye Şubesi Hazine Müsteşarlığının denetimine tabiidir.

UK8124-MD 09/22