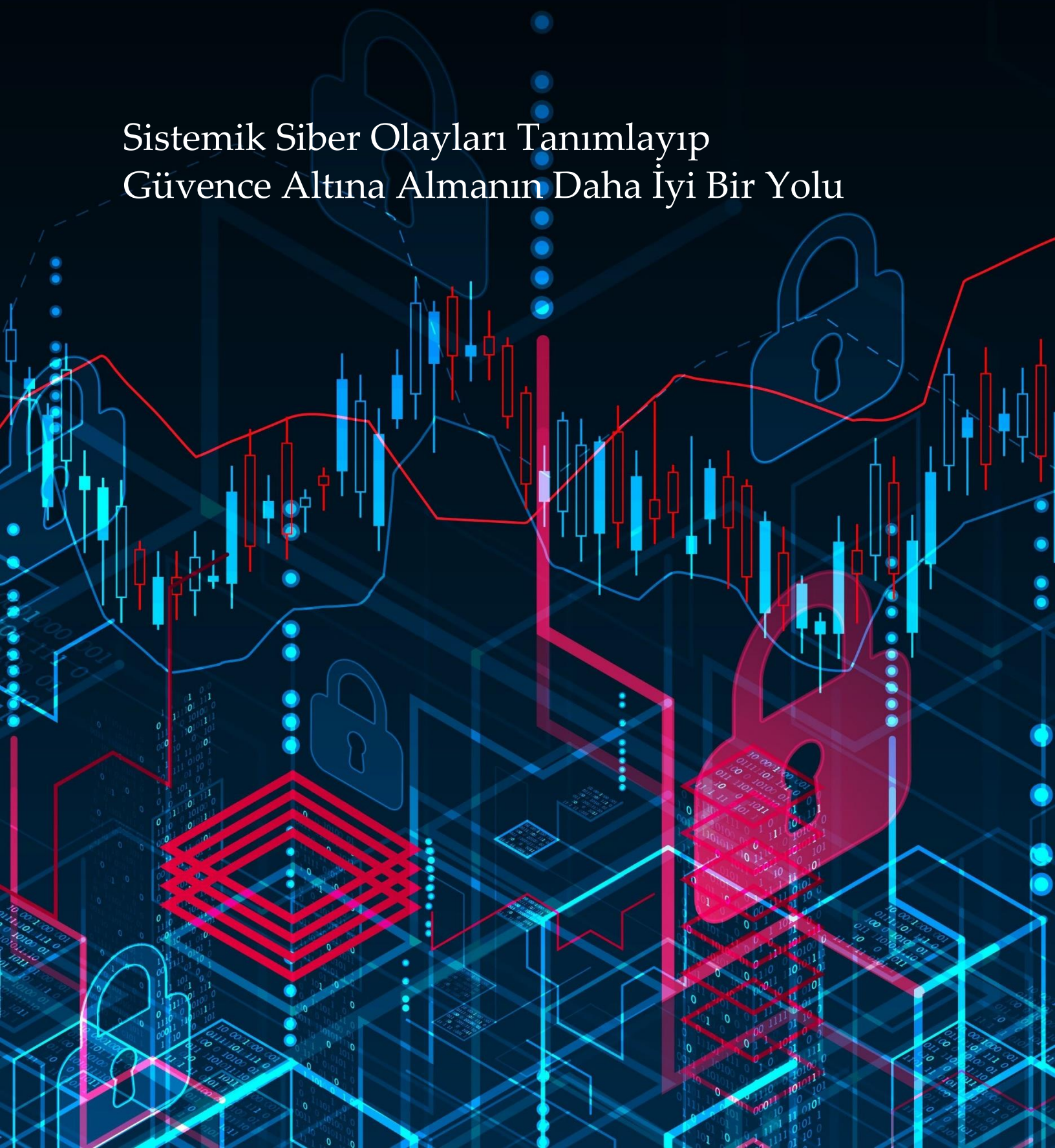
CHUBB®

Sistemik Siber Olayları Tanımlayıp Güvence Altına Almanın Daha İyi Bir Yolu



Giriş

Katastrofik bir siber saldırının çok büyük maddi hasara yol açma potansiyeli bilinse de henüz tam olarak anlaşılmış değil. Sonuç olarak birçok şirket siber dayanıklılığını artırmaya çalışırken sigorta sektörü de bu riskleri yönetmek adına çözümler geliştiriyor.

Tüm bu çabalara rağmen, kuruluşların ve tüketicilerin teknolojiye olan bağımlılığının giderek artması, teknolojik alt yapılarla birbirine bağlanması,
siber risklerin katlanarak arttığı bir ortam yaratmıştır. Tıpkı pandemiler gibi siber-CAT olaylarının da coğrafi sınırları veya geçici kısıtlamaları yoktur.

Risk altındaki kuruluşlar, hükümetler, sigorta şirketleri, brokerler ve siber güvenlik sektörü dahil olmak üzere tüm paydaşların, kuruluşlara ve bireylere ihtiyaç duydukları sigorta teminatı sağlamaya devam ederken genel ekonomik istikrarı ve toplumsal dayanıklılığı koruyacak çözümler geliştirmesi ve uygulaması gerekmektedir.

Sigorta sektöründe uzun vadeli sürdürülebilirliğin önündeki engellerden biri sistemik siber olaylara ilişkin tutarlı ve net bir tanımın olmamasıdır. Müşterilerin sigorta teminatının kapsamını bilmesi ve sigortacıların, üstlendikleri müşteri risklerinin yükümlülüklerini yerine getirebilmesi adına risk yöneticileri, brokerler ve sigortacılar poliçe hüküm ve koşullarına dair ortak bir anlayışa nasıl varabilirler?

Aşağıdaki Soru-Cevap bölümünde, Chubb Group ve Global Siber Risk Bölüm Başkanı, Michael Kessler, genel yanlış anlaşılmalar ve çözümler de dahil olmak üzere yaygın siber risklere yönelik olarak gelişmekte olan sigorta piyasasından bahsediyor.

Michael Kessler ile Soru-Cevap

S: Sistemik risk nedir? Nasıl tanımlanmalıdır?

C: Siber sigorta piyasasında, “sistemik risk” kavramına dair net bir tanım bulunmuyor. Chubb olarak, siber güvenlik bağlamında “sistemik” olayı şöyle tanımlıyoruz: Genellikle kötüye kullanılan tek bir hata noktası olmak üzere, ortak unsurlar veya müştereklikler sebebiyle çok sayıda müşteriye geniş çaplı
zarar verebilecek olan bir olay.” Daha basit bir şekilde ifade etmek gerekirse, tek bir olayla birden fazla kuruluşu etkileyen siber vaka olarak tanımlayabiliriz. Binlerce işletme tarafından kullanılan bir dosya aktarım yazılımdaki güvenlik açıklığından faydalanılarak kötü amaçlı yazılım yerleştirilmesi, verilerin çalınması veya işletmede aksaklığa sebep olunması, sistemik olaylara örnek olarak verilebilir. Bu şekilde tek bir istismar sebebiyle çok fazla müşterinin kayıp yaşaması, felaket düzeyinde kayıplara sebep olabilir.

SİSTEMİK RİSKİN TANIMI:

Tek bir olayla birden fazla kuruluşu etkileyen siber vaka.

S: Siber sigorta piyasası, giderek artan münferit fidye yazılım saldırılarına ve sistemik olaylara nasıl cevap veriyor?

C: Genel anlamda piyasa, fidye yazılım olaylarının şiddeti ve sıklığı sebebiyle meydana gelen hasar maliyetlerindeki değişime ayak uydurmak adına, risk ortamındaki değişiklikleri takip ediyor. Sistemik riske verilen yanıtlar artık daha üstü kapalı.

S: Siz ve ekibiniz, sistemik riske dönüşüm hakkında ne düşünüyorsunuz?

C: Chubb olarak, sektörün sistemik siber riski ele alma şekline ilişkin üç adet sorun tanımlamış bulunuyoruz: 1) Sigortalılara yönelik kapsamda netlik olmaması; 2) Riskin yetersiz şekilde fiyatlandırılması; 3) Riskin izlenmesine yeterli düzeyde odaklanılmaması.

BU KONUDA ÜÇ ZORLAYICI KONU

- Sigortalılara yönelik kapsam netliğinin olmaması
- Riskin yetersiz şekilde fiyatlandırılması
- Riskin izlenmesine yeterince odaklanılmaması

Birinci sorunu çözmek adına, yaygın siber olay kavramını net bir şekilde tanımlamak istedik. Bu bağlamda sistemik olay, tek bir eylemden ortaya çıkan ve bu tek eylemin, siber riske özgü geniş etki potansiyelini açığa çıkaran bir durumdur. Poliçe açıklaması net ve kesin olduğunda, yüksek maliyetli davalar hafifletilebilir ve sigorta şirketleri daha fazla kapasiteyi uzun dönemde tutarlı sunabilir.

İkinci olarak; poliçemizi, sigortalıların sistemik kapsamların fiyatlandırmasını şeffaf bir şekilde görebileceği ve risk toleransları doğrultusunda, satın alınacak limit ve konservasyon konusunda aktif karar verebileceği şekilde tasarladık. Bu, sigorta ürünleri açısından bilindik bir konsept olup; deprem kapsamının, mülkiyet poliçesindeki diğer tüm risklerden ayrı şekilde alınması buna örnek verilebilir.

Üçüncü olarak, modelleme firmalarıyla iş birliği yaparak hasar senaryolarını poliçe tanımlarıyla uyumlu hale getirdik; böylelikle, bu riske ilişkin daha tutarlı ve odaklı bir bakış açısı sunmuş olduk.

S: Chubb poliçesinin kapsadığı ve kapsamadığı yaygın olaylar nelerdir?

C: Savaş veya altyapı bozulmasını içerenler hariç olmak üzere yaygın olaylar kapsam dahilinde olup, sigortalı tarafından satın alınan limit ve konservasyona tabidir. Bu kapsamın dışında kalan başka bir şey yoktur. Yaygın bir olay meydana gelirse ve savaş ilanı ya da altyapı kaynaklı bir sebep yoksa işletmeler, sigorta kapsamında olduklarını bilerek rahat edebilirler. Savaş veya altyapı bozulmasından kaynaklanan siber olaylar kapsam dışıdır. Ayrıca, savaş ve altyapı kavramları poliçede net ve objektif bir biçimde tanımlanmıştır; böylece sigortalıya, herhangi bir hasar meydana gelmeden önce sözleşmede netlik sağlanır. Kapsam, bir saldırının failinin sonradan değerlendirilmesine bağlı olmadığından (örneğin, 'devlet destekli' veya 'devlet destekli' saldırganlar) herhangi bir belirsizlik söz konusu değildir.

S: Peki ya reasürans konusu?

C: Reasürans, uzun yıllardır olduğu gibi günümüzde de büyük ölçüde bir kotpar piyasası hakim durumunda. Bunun yüzeysel anlamı, sigorta şirketinin, primin bir kısmını ve hasarından aynı oranı reasürörlere devretmesidir. Bununla birlikte, çoğu sözleşme reasürörlerin hasarları için bir üst sınır içermekte, bu da sedana bu hasarları ödeyecek primi olmadan önemli hasar riski bırakmaktadır. Sermayenin daha etkin bir kullanımında ise reasürörler, hasarı olay bazını aşan hasar limitine siber riski güvence kapsamına alır. Bu, sigorta şirketini tek bir CAT olayından kaynaklanan kümül hasara karşı koruyan katastrofik hasar fazlası reasüransı ile çalışan modele benzer. Bu yaklaşım sayesinde reasürörler, orantılı olarak daha az sermaye kullanımıyla sigorta süresi dışı volatilite konusunda daha büyük marjlar elde edebiliyor. Reasürörlerin özsermaye kârlılığı (ROE) artıyor ve siber sigorta piyasasının geneli daha verimli hale geliyor. Reasürans piyasasının gelişmesi için sistemik siber olayın ne olduğuna dair net bir tanıma ve bu olayların sıklık ve şiddetini modellemek için tutarlı bir yaklaşıma ihtiyacı vardır. Hem Chubb politikası hem de dünyanın en büyük siber sigortacılarından oluşan bir endüstri konsorsiyumu olan CyberAcuView tarafından yayınlanan politika, sistemik bir olayın net bir tanımını sunmaktadır ve modelleme firmaları son 12 ay içinde modellemelerinin kalitesini ve tutarlılığını büyük ölçüde geliştirmiştir.

NETLİĞİN DEĞERİ:

Fiyatlama modellerinin kalitesi ve tutarlılığı geçtiğimiz 12 ay içinde ciddi anlamda iyileşme göstermiştir.

S: Pazarda poliçe şartlarının açıklamasına verilen tepki ne oldu?

C: Chubb'ın poliçe şartlarının tanıtmasının üzerinden neredeyse iki yıl geçti. Birçok müşteri Chubb'ın yaptığı şeyi anlıyor ve kesinlikle destekliyor. Kendilerinin risk yönetimi konusunda daha bilinçli kararlar almasına yardımcı olunmasında net olmanın değerini görüyorlar. Örneğin büyük bir işletme, poliçesine sadece katastrofik riskleri dahil edip, daha az mali risklere sigorta kapsamına almayı tercih edebilir. Büyük bir şirket ise, fidye yazılım saldırısından kaynaklanan düşük maliyetli kayıpları bilançosuna koyup, kontrol edemediği riskler için sigorta yaptırmaya karar verebilir.

S: Chubb'ın yaklaşımının daha geniş kapsamlı şekilde kullanılması gerektiğini düşünüyor musunuz?

C: Chubb, dünyada siber sigorta alanında en büyük hizmet sağlayıcılardan birisi. Poliçe sahipleri için yirmi yıldan uzun süredir siber riskler konusunda çalışıyoruz. Tüm engelleri aşmak için lider olmaya odaklanmış durumdayız. Bu deneyimlerimizi, verilerimizi ve içgörülerimizi kullanarak, bu büyüyen riski karşılamak adına çözümler geliştirmeye devam edeceğiz. Modellememiz müşterilerimize anlamlı koruma sunacağından ve başka sigortacılara da örnek teşkil edeceğinden eminiz. Daha homojen kapsamların sunulması ve sigorta sözleşmelerine potansiyel olarak farklı limit, kesinti ve fiyatlandırmaların dahil edilmesi, sigortalı adaylarına ve reasürörlere önemli faydalar sağlar.

SEKTÖR İÇİN MODELLEME:

Daha homojen kapsamların sunulması ve sigorta sözleşmelerine potansiyel olarak farklı limit, kesinti ve fiyatlandırmaların dahil edilmesi, sigortalı adayları ve reasürörler önemli bir fayda yarattı.

Katastrofik riskler çoğalıyor

Sistemik bir siber olayın felaket boyutunda bir kayba neden olma potansiyeli korkutucu düzeyde olup,riski de giderek büyümektedir. 2022 yılında, dünya genelinde kötü amaçlı yazılım saldırılarının sayısı, 2021'deki toplam hacimden neredeyse beşte iki daha fazla olmuştur. Bu oran 2022'nin dördüncü çeyreğinde en yüksek noktaya ulaşmış; işletme başına haftada 1.168 saldırı rapor edilmiştir.[1]

2022 yılında yazılımlarda 25.000'den fazla güvenlik açıklığı tespit edilmiş olup, bu değer bugüne kadar rapor edilen en yüksek yıllık rakamdır.[2] Güvenlik açığı, yazılımda bulunan ve kötü amaçlı yazılımlar tarafından istismar edilebilen bir kusur veya zayıflıktır. Nisan, Mayıs ve Haziran 2023'te, Ulusal Standartlar ve Teknoloji Enstitüsü yazılımlarda toplam 6.991 güvenlik açığı tespit etmiş, bunların 1.027 tanesi "kritik" olarak sınıflandırılmıştır.[3]

Felaket boyutunda kayıplara neden olan sistemik bir olaya ilişkin tahminler, global sigorta piyasasının toplam kapasitesini aşmaktadır.[4] Hükümet Mali Sorumluluk Birimi (GAO) tarafından yayımlanan bir raporda bu olaylar, "ilk hedeften ekonomik olarak bağlantılı firmalara yayılarak hasarı büyüten" siber olaylar olarak tanımlanmaktadır. GAO raporunda, tek bir sistemik siber olaydan kaynaklanan potansiyel zararın 2,8 milyon ile 1 trilyon dolar arasında olduğu tahmin edilmiştir.[5]

Chubb'ın Siber İşletme Risk Yönetimine Yaklaşımı

Yaygın Olaylar da dahil olmak üzere çok çeşitli siber olayların ele alınmasına yönelik sürdürülebilir bir yaklaşım

Chubb'ın Siber ERM'sinin üç ana hizmeti

- Kayıp Azaltma Hizmetleri – herhangi bir olay meydana gelmeden önce siber güvenlik risklerine ilişkin önemli alanları ele almaya ve belirlemeye yönelik araçlar ve kaynaklara erişim.
- Olay Müdahalesi Hizmetleri – bir olay meydana geldiğinde kayıp risklerinin sınırlandırılmasına yardımcı olacak; hukuk, adli bilişim, bildirim, çağrı merkezi, halkla ilişkiler, dolandırıcılık danışmanlığı, kredi izleme ve kimlik telafi hizmeti gibi alanlarda uzmanlık sahibi kişilerden oluşan geniş çaplı bir ekip.
- Risk devri – Chubb'ın finansal gücüyle desteklenen kapsamlı ve sürdürülebilir sigorta teminatı.

Rekabet avantajları

- 1998'de ilk ürünü piyasaya sürüldüğünden beri siber risk çözümleri alanında lider sağlayıcı.
- Ölçek, sektör veya risk türü fark etmeksizin müşterilerin özel ihtiyaçlarını karşılamaya yönelik yenilikçi ve yüksek düzeyde özelleştirilebilir risk çözümleri.
- Asgari prim ödemesi olmaması. Teminat ve limitler kapsamına göre tüm risk boyutları için primler ölçeği.
- Siber suç teminatı, zeyil yoluyla veya Chubb'ın sektör lideri Sadakat ve Suç ürünlerinden ayrı poliçeler altında sağlanır.
- Asgari düzenleyici gerekliliklerinden daha sağlam nitelikteki geniş kapsamlı tüketiciye dayalı çözümler içeren Siber Olay Müdahalesi Masrafları.
- Uygun nitelikteki küçük riskler için çevrim içi fiyat teklifi ve gerçek zamanlı poliçe tanzimi. Bahsedilen riskler için Chubb sigortacınız olarak hızlı geri dönüşler sağlayacaktır.
- Değişen mevzuat, hukuk ve siber güvenlik standartlarını kapsayacak ve ileriye dönük değişiklikleri de göz önünde bulunduracak şekilde tasarlanmış yenilikçi teminat
- Süreç boyunca karar vermeye yardımcı olmak için tipik siber olay akışlarıyla uyumlu hale getirilen kolay okunur formlar.
- Barındırma ve veri depolamanın devamlı değişen yapısına yönelik dünya genelinde uygulanabilir Teminat Bölgesi

Yaygın olay zeyilnamesi

- Yaygın Olay Zeyilnamesi, Sigortalı ile hiçbir ilişkisi olmayan tarafları etkileyen ve yaygın bir etkiye sahip olan olayları kapsar. Sel ve deprem risklerinin yangın sigortaları dahilinde ele alınmasına benzer şekilde teminat, limitler, konservasyonlar ve koasürans tüm Yaygın Olaylar için veya özel riskler itibarıyla özelleştirilebilir:
  - Yaygın ve Ciddi Nitelikteki Güvenlik Açıkları
  - Yaygın ve Ciddi Sıfır Gün Güvenlik Açıkları
  - Yaygın Yazılım Tedarik Zinciri Güvenlik Açıkları
  - Diğer tüm Yaygın Olaylar
- Fidye Yazılımı Olayları Zeyilnamesi tüm siber teminatlarda aynı şekilde uygulanacak özelleştirilmiş bir teminat, limit, konservasyon ve koasüransa olanak tanıyarak giderek artan fidye yazılımı riskini ele alır.
- İhmal Edilen Yazılım Güvenlik Açığı Zeyilnamesi, 45 gün boyunca tam kapsamlı bir teminat sağlayarak iyi bir yazılım yamalama korumasını takdir eder ve ödüllendirir ancak 45 gün sonrasında halen yamalanmamış yazılımlarda ise Sigortalı ile Sigortacı arasındaki risk paylaşımını zaman geçtikçe kademeli olarak yeniden değerlendirir.

[1] Check Point. Küresel Siber Saldırılar 2022'de %38 Artış Gösterdi. 9 Ocak 2023.
[2] Tenable Research. Boşluklara Dikkat: 2022'de Açıklanan Güvenlik Açıklarına Yakından Bir Bakış.
[3] NIST Ulusal Güvenlik Açığı Veri Tabanı. Wall Street Journal haberi, 20 Haziran 2023
[4] Marsh. Siber Sigorta Pazarına Genel Bakış, 2021 Dördüncü Çeyrek.
[5] ABD Devlet Hesap Verebilirlik Ofisi. Yıkıcı Siber Olaylara Yönelik Potansiyel Federal Sigorta İşlemleri. 29 Eylül 2022