Siber Sistemik Risk/Ürün Güncellemesi:

Broker SSS'lar

CHUBB®

Ekim 2021

Chubb, siber sigorta sektörünün uzun dönemde sürdürülebilir olmasına yardımcı olacak yönlendirme ve yapılandırmayı sağlayarak sektöre hız kesmeden liderlik etmeye odaklıdır.

Günümüzde siber olayların sıklığı ve şiddeti, Chubb da dahil birçok sigortacıyı fiyat politikaları ile şart ve koşullarını değerlendirmeye yöneltiyor. Geçtiğimiz aylarda yazılım tedarik zinciri ve e-posta güvenlik sağlayıcılarından veri sunucularına ve altyapıya kadar uzanan çeşitli hedefleri tehlikeye atan birçok yaygın nitelikte siber olay meydana gelmiştir. Bu olaylar, felaket niteliğindeki olaylara dönüşme potansiyeli olan birçok siber saldırı türünü içeriyordu.

Sonuç olarak Chubb, bu riskleri yönetmeye yönelik yeni ve yenilikçi çözümler geliştirmektedir. Chubb, poliçe sahiplerimizin ve satış kanallarımızın bildiği ve anladığı temel siber teminatları sunmaya devam edecek olmakla birlikte halihazırda yaygın olaylara ilişkin şart ve koşullarımızı da yeniden yapılandırıyor ve aynı zamanda tüm taraflar için daha fazla bilgiye dayalı bir teminat netliği sağlayabilecek farklı çözümler hakkında sektörel birlikler ve hükümetlerle iş birliği yapıyor.

Satış Kanalları ve Poliçe Sahipleri Üzerindeki Etki

Chubb olarak yeni çözümlerimizin satış kanalları için siber sigorta pazarında daha iyi ve uzun vadede istikrarlı bir büyüme sağlayacağını düşünüyoruz. Brokerler, sistemik riskler için teminatın net bir şekilde belirlenmesi, poliçe şartlarını müşterisinin özel risklerine göre özelleştirme ve katma değerli hasar azaltma ve risk danışmanlık hizmetleri ile teminatların içeriğini ve sayısını artırmada dahil olmak üzere bu alandaki uzmanlıklarını gösterebilecekleri bir fırsata sahip olacaklar. Chubb'ın yeni yaklaşımı, sabit kıymet sigortası konusunda deneyimli broker ve müşterinin aşina olduğu kavramlardan yararlanacaktır. Zaman içinde, siber riskleri ölçmeye yönelik yapılandırılmış bir yaklaşım pazarda daha fazla siber sigorta kapasitesi oluşturacaktır.

Siber Risk Pazarı

Siber sigortaya ilişkin mevcut strateji değişikliklerini yönlendiren nedir?

Siber saldırılar ve tehditler her geçen gün artıyor. 2020'de 18.000'den fazla yeni yazılım güvenlik açığı yayınlanmış olup bu sayı, 2015'teki sayının neredeyse üç katıdır ve giderek artmaya da devam etmektedir.[1] Öte yandan, 2020'de yaklaşık 1,2 milyon yeni kötü amaçlı yazılım tehdidi tespit edilmiş olup, bu da 2015'te belirlenen sayının iki katından fazladır.[2] Fidye yazılımı gibi taktikler daha yaygın ve maliyetli olmakla beraber işle ilgili e-posta tehditleri ve veri ihlalleri, özellikle uzaktan çalışma modeli ile birlikte, siber saldırı görülme sıklığını hiç olmadığı kadar yüksek seviyelere taşımaya devam etmektedir. Bu nedenle siber olayların artan sıklığı ve şiddeti, sigorta şirketlerinin hasar oranlarını baskılarken, potansiyeli olan sistemik riskler de her zamankinden daha yaygın hale gelmektedir.

Diğer kuruluşlar sistemik siber risk konusunda Chubb ile aynı bakış açısına sahip mi?

,bu konunun önemi ve aciliyetinin farkında olduğuna inanıyoruz. 2020'de ABD Kongresi, Senatör Angus King (Bağımsız-ME) ve Temsilci Mike Gallagher (Cumhuriyetçi-WI) başkanlığında Siber Alem Solaryum Komisyonunu kurdu. Bir yıl süren bir çalışmanın ardından Komisyon, ABD'nin çok ciddi bir siber saldırı riski altında olduğu ve "siber ortamda tehlikeli derecede korunmasız" olduğu sonucuna vardı.[3]

Avrupa'da, 15 yılı aşkın bir süre önce, kamu sektörünü ve özel sektörü etkileyen ve sayıları giderek artan ciddi siber saldırılara karşı mücadele için Avrupa Birliği Siber Güvenlik Ajansı (ENISA) kurulmuştur. Bu ajansın Nisan 2021'de yayınladığı yeni raporda, günümüzdeki siber güvenlik tehditleri göz önüne alındığında, kuruluşların kritik bilgi ve bilgi teknolojisi (ICT) varlıklarını etkin bir şekilde koruyabilmeleri için küresel siber güvenlik iş gücünün %89 oranında artması gerektiği vurgulanmaktadır. Bu kritik durumu ele almak üzere hükümetler çok sayıda program ve politika uygulamaya başlamıştır.

Birleşik Krallık'ta, Savunma Bakanı Ben Wallace Ekim ayında yaptığı bir açıklamada Birleşik Krallık'ın siber saldırılara karşı dayanıklılığını artırmak için ülkede yeni bir dijital güvenlik merkezi kurulduğunu belirtmişti.

Buna ek olarak, sigorta derecelendirme kuruluşu AM Best Haziran 2021'de "siber sigorta pazarının geleceğini ümitsiz" gördüğünü belirterek bu anlamda "siber risklerin zincirleme etkilerinin coğrafi veya ticari sınırların olmayışının geniş kapsamlı sonuçlarına" dikkat çekmiş ve "siber güvenlikle ilgili risk yönetim yaklaşımı eksik olan sigortacıların risk toleranslarını aşan bir risk birikimiyle karşı karşıya kalabileceklerini ve derecelendirme baskısı yaşayabileceklerini" de sözlerine eklemişti.[4]

Diğer kuruluşların gözlemlerine erişmek için lütfen aşağıda verilen bağlantıları ziyaret edin:

- Ulusun Siber Güvenliğini İyileştirme Hakkında Başkanlık Kararnamesi (ABD Hükümeti): www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Siber Sigorta: Sigortacılar ve Poliçe Sahipleri Sürekli Değişen bir Pazarda Zorluklarla Karşı Karşıya (ABD Hükümeti Sorumluluk Ofisi): www.gao.gov/products/gao-21-477
- Siber Sigorta Oranları 2021'de %50 Artabilir (MarshMcLennan Agency): www.marshmma.com/blog/cyber-insurance-rates-could-rise-50-in-2021
- Daha İyi Kararlar Alarak Risk ve Fırsatların Dengelenmesi (Aon): www.aon.com/2021-cyber-security-risk-report/

Sektörle kıyaslandığında Chubb'ın stratejisi nasıl?

Siber sigorta sektörünün büyük bir bölümü; fidye yazılımı ve oran yeterliliği gibi daha dar kapsamlı konulara odaklanmıştır ve kapasiteyi düşürmek, oranları artırmak ve sektöre ya da teminata özel düzenlemeler yaparak süreci yönetmektedir. Chubb da benzer şekilde değerlendirmeler yapmanın dışında onlarca yıllık deneyimini ve önemli ölçüde büyük faaliyet alanlarından faydalanarak sistemik risklere ilişkin büyük resme de odaklanıyor. Diğer kuruluşlar sektörümüzde bu konuya duyulan ihtiyaçtan bahsetmiş olsa da bugüne kadar kayda değer çok az eylemde bulunulmuştur. Chubb bu alanda liderlik yapmayı hedeflemektedir.

Gelişmiş siber sigortalama teknikleri siber felaketlere ilişkin riskleri azaltabilir mi?

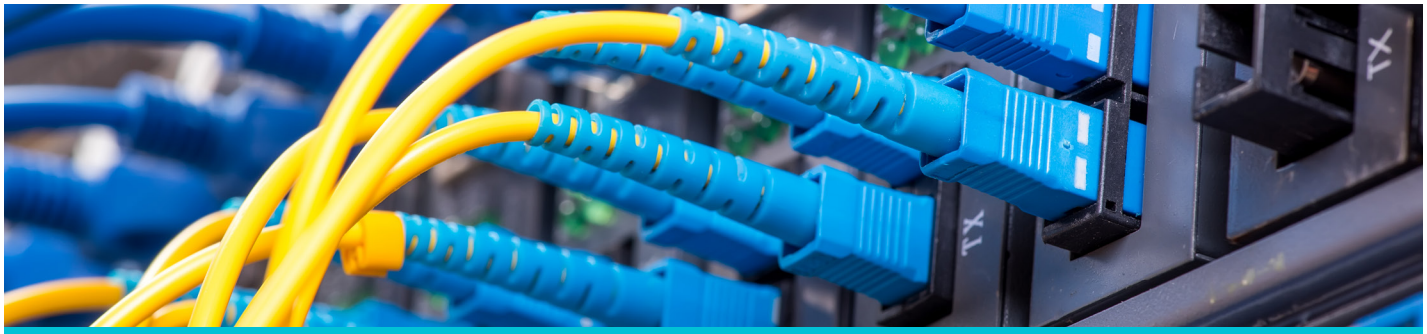
Chubb olarak Siber risk mühendisleri ve bu konuda uzman sigorta uzmanlarından oluşan özel bir ekibe sahibiz. Sigortalama süreçlerimizde yeni tehdit analizi ve yapay zeka araçlarını uygulamaya koyuyoruz. Ayrıca, siber poliçe sahiplerinin hasar önleme ve azaltma hizmetlerinden oluşan kapsamlı bir pakete erişmelerini de sağlıyoruz. Bu alanlardaki proaktif yatırımımız, Chubb'ın siber sigortalama çıktılarının siber sigorta sektörünün genelinden daha üstün bir performans göstermesini sağlamıştır.[5] Bu önemli yatırımlara rağmen özellikle iç kontrolleri ve en iyi uygulamaları atlatmak için birçok siber tehdit geliştirilmiştir. Hiçbir sigortalama veya hasar önleme kontrolü siber saldırıya uğrama riskini tamamen ortadan kaldıramaz.

Sistemik siber risk nedir? Chubb bu terimi nasıl tanımlıyor?

Bize göre "sistemik" kelimesi, içinde barındırdığı ortak noktalar veya ortak risk unsurları nedeniyle birçok müşteriyi etkileme potansiyeline sahip bir riski ifade ederken "felaket niteliğindeki" kelimesi ise birçok poliçe sahibi için ciddi veya büyük kayıplara yol açan sistemik bir riski ifade eder.

Son yıllarda ne gibi felaket niteliğinde siber riskler ortaya çıkmıştır?

Kurumlar ve tüketicilerin giderek artan orandaki teknoloji bağımlılığının yanı sıra teknolojiler ile ortakların birbirine bağlı olması, siber risklerin katlanarak büyüyebileceği bir ortama zemin hazırladı. Siber olayların aynı zamanda daha yaygın bir etkisi de vardır. Aralık 2020 ile Mart 2021 arasındaki 100 günlük süre içinde gerçekleşen birçok büyük çaplı saldırı, yazılım tedarik zinciri ve e-posta güvenliği sağlayıcılarından veri sunucularına ve belediye altyapısına kadar çeşitli hedefleri tehlikeye atmıştır. Dünyanın dört bir yanında toplamda 100.000'i aşkın kuruluş bu olaylardan etkilenmiş ve bu durum milyonlarca müşteri ve vatandaşı etkileyen aksamaların yanı sıra ciddi ekonomik kayıplara da neden olmuştur. Örneğin, güvenilir bir ağ analizi yazılımının güncellemesine yerleştirilen kötü amaçlı bir kod üzerinden gerçekleşen Solorigate yazılım tedarik zinciri saldırısı 20.000 şirket ve devlet kurumunu etkilemiştir. Saldırıdaki amaç, kritik verileri veya diğer bilgileri çalmak veya imha etmek olsaydı bu durum çok daha kötü sonuçlanabilirdi.n.



Aşağıdaki risk türlerinin, özellikle kombinasyon halinde karşımıza çıktığında felaket niteliğinde olaylara dönüşme potansiyeline sahip oldukları tespit edilmiştir:

Bilinen Ciddi Güvenlik Açıkları:

Yama uygulanmayan bazı bilinen yazılım güvenlik açıkları; suistimal edilmelerinin kolay olması, sınırlı erişim öncelikleriyle uzaktan dağıtılabilmesi ve önemli olumsuz etkilere sebep olabilmeleri nedeniyle ciddi sonuçlar doğurabilir.[6]

Ciddi Sıfır Gün Güvenlik Açıkları:

Siber suçlular tarafından bilindiği halde henüz başkaları tarafından bilinmeyen; kolayca suistimal edilebilen, potansiyel olarak ciddi nitelikteki ve çoğu zaman koruma içermeyen bazı yazılım güvenlik açıkları.

Yazılım Tedarik Zinciri Güvenlik Açıkları:

Bu saldırılar temelde kötü niyetli kişilerin güvenilir, sertifikalı yazılımlar aracılığıyla sistemlere girmesine izin veren bir Truva atından doğar.

Altyapı Kesintileri:

Elektrik şebekeleri ve telekomünikasyon hizmetleri gibi kritik toplumsal altyapılar; sistem arızaları, insan hataları veya programlama hataları da dahil olmak üzere siber saldırı veya kötü amaçlı olmayan siber olaylar nedeniyle çok büyük ölçekte olası arıza riskiyle karşı karşıyadır. Bu yılın başlarında gerçekleşen ve ABD'nin doğu kıyısına hizmet veren benzin tedarik şirketi Colonial Pipeline'ı hedef alan saldırıda bir fidye yazılımı yoluyla bir altyapı kesintisinden yararlanılmış ve bu da birçok eyalette milyonlarca vatandaş ve işletme için benzin kıtlığına neden olmuştur.

Diğer 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 günümüzde kritik toplumsal altyapılar haline gelmiş ve bazı büyük bulut bilişim firmaları o kadar yaygın olarak kullanılmaktadır ki yaşanacak bir kesinti binlerce, hatta belki de milyonlarca şirketin faaliyetlerini etkileyebilir.

Fidye Yazılımı Olayları:

Yapısı gereği tam olarak sistemik niteliğinde olmasalar da hedeflenen kuruluşların veya kişilerin elektronik dosyalarını veya bilgilerini bir ücret ödenene kadar rehin tutan fidye yazılımı saldırıları artık otomatik bir etkinlikle gerçekleştirilmekte ve fidye talepleri de sürekli olarak artmaktadır. NotPetya ve WannaCry olayları gibi bazı yıkıcı saldırılar fidye yazılımı gibi görünebilir.

Siber sigorta pazarı yıllardır fidye yazılımını konuşmaktadır. Chubb artık buna farklı mı bakıyor?

Birkaç yıldır fidye yazılımı trendlerini analiz etmekteyiz; bu trendler değiştikçe sigortalama stratejilerimiz de değişmiştir. Riskleri yönetmeye yardımcı olmak için sigortalama stratejisi değişiklikleri (örn. belirli kontrollere sahip olmayan belirli kategoriler veya işlerden kaçınma) gerçekleştirmenin yanında konservasyonlar, limitler ve koasürans alanlarında da değişiklikler yaptık. Chubb aynı zamanda bu risklere yönelik, müşteriler ve potansiyel müşteriler için risk faktörlerini tespit etmemize yardımcı olması açısından çeşitli iç ve dış kaynaklardan alınan risk sinyallerini ve ağırlıklı faktörleri analiz eden sinyal tabanlı bir sigortalama da uygulamaktadır. Chubb'ın yeni siber ürün teklifleri, birden fazla sigorta sözleşmesinde fidye yazılımıyla karşılaşılan durumlar için alt limitlerin, koasüransın ve konservasyonların yapılandırılmasına yönelik daha da fazla yöntem sunacaktır.

Chubb şu ana kadar kaç tane sistemik siber risk hasar bildirimi almıştır?

Chubb, son dokuz ay içinde büyük, yaygın siber olaylarla ilgili yüzlerce siber bildirim almıştır.

Siber pazarda neden bu kadar çok değişiklik görmeye devam ediyoruz? Sigorta sektörü, diğer iş kollarında da benzer çalkantılar yaşadı mı?

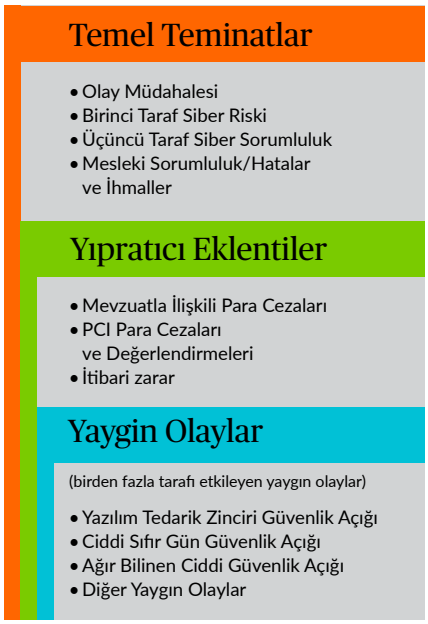
Siber sigorta daha henüz geçtiğimiz yıllarda bir segment olarak ciddi anlamda olgunlaşmış olupşimdi bile büyük ölçüde gelişmekte olan bir teminat alanıdır. Aynı zamanda, siber riskler dinamik bir yapıda olup karmaşıklık ve şiddet bakımından hızlı bir artış göstermektedir. Geçmişte, mal sigortası pazarı, 1906 San Francisco depremi ve 11 Eylül terör saldırıları gibi benzeri görülmemiş ölçekte ani olaylardan kaynaklanan şoklar yaşadı. Çözümler ancak bu olayların yaşanmasından sonra geliştirildi ve böylece, belirtilen tehlikeler konusunda daha fazla netlik oluşturularak felaket niteliğindeki riskler için ayrı teminatlar sağlandı. Siber sigorta sayesinde, genel ürün tasarımını iyileştirmek ve aynı zamanda sigorta piyasası için istikrar ve müşteriler için de teminat netliği sağlayabilecek şekilde hükümetlerle muhtemel çözümler oluşturmak üzere harekete geçme fırsatına da sahibiz.

Chubb'ın Siber Ürün Teklifi

Chubb şu anda sunmakta olduğunuz siber teminatların aynılarını sunmaya devam edecek mi?

Şu anda sunduğumuz temel teminatların aynıları (olay müdahale masrafları, birinci taraf siber riski, üçüncü taraf siber sorumluluğu ve mesleki sorumluluk) mevcut olmaya devam edecektir. Chubb ayrıca Sınırlı Etkiye Sahip Olaylar ile Yaygın Olaylar arasında bir ayrım yapmaktadır. Temel ürünlerimizin, standart Sınırlı Etkiye Sahip Olay teminatları kapsamında geçmiş kayıpların tahmini olarak %90'ını karşılayacağını öngörüyoruz.

Chubb, önemli yıpratıcı riskleri teminat altına almakla birlikte ana siber sigorta ürününün eklentileri olarak, bu teminatları daha yapılandırılmış ve sürdürülebilir bir şekilde sağlayabilmemiz için yaygın ve yıkıcı potansiyeli olan sistemik risklere yönelik ek teminatlar da sunacaktır. Bunlar toplu olarak Yaygın Olay teminatları olarak adlandırılacak olup poliçede ana hatlarıyla belirtilmiş çeşitli alt bileşenleri içerecektir. Yaygın Olaylar ve her bir alt bileşen özel bir limit, konservasyon ve koasürans miktarına tabi olacaktır. Bu yöntem, mal sigortasının yüzyılı aşkın süredir sel ve deprem gibi felaket niteliğindeki riskleri ele alma biçimine benzemektedir.



Ne tür teminat eklentileri beklemeliyiz?

Chubb, daha önce yalnızca zeyilname yoluyla eklenen temel siber sigorta ürünü içindeki birçok teminat geliştirmesini kapsam içine alacaktır. Bunlar; mevzuattan kaynaklanan para cezaları, Ödeme Kartı Sektörü (PCI) para cezaları ve değerlendirmeleri, itibari zarar, aldatıcı nitelikteki havalelere ilişkin dolandırıcılıklar, önleyici kapatma ve benzeri yıpratıcı eklentileri içerir. Chubb aynı zamanda yazılım tedarik zinciri suistimalleri, ciddi sıfır gün suistimalleri ve bilinen ciddi güvenlik açığı suistimalleri gibi Yaygın Olayları karşılamak için ayrı teminat eklentileri de sunacaktır. Soldaki grafik bu listeye genel bir bakış sunar. Müşteriler ve potansiyel müşterilerin, brokerleri ile birlikte çalışarak operasyonlarında ve BT ortamlarında karşı karşıya kalabilecekleri kendilerine özgü siber riskleri belirlemeleri ve ardından kendileri için en anlamlı olan teminat eklentilerini seçmeleri gerekecektir.

Chubb'ın siber teminatlara ilişkin fiyat politikası değişecek mi?

Fiyatlandırma her müşterinin özel teminat ihtiyaçlarını ve risk profilini yansıtmaya devam edecektir. Kabul edilme esasına göre sigorta yapılabilmesi için yargı onayının gerekli olduğu durumlarda güncellenmiş bir oran beyanı yapılacak olup işleri söz konusu onaylanmış oran beyanlarına göre sigortalayıp yine bu şekilde fiyatlandıracağız.

Bu ürün değişiklikleri ne zaman yürürlüğe girecek?

Chubb halihazırda büyük hesaplarda bu yeni yaklaşımı kullanmaktadır ve önümüzdeki aylarda diğer pazar segmentlerine de açılacaktır. Bu doğrultuda, müşterinin özel risklerini belirlemek ve onlar için doğru korumayı sağlayacak teminat eklentilerini tespit etmek için müşterinizin yenilemelerinden önce risk yöneticileriyle çalışmaya başlanması kritiktir. Yeni yaklaşımın kabul edilme esasına göre uygulanması, Ocak 2022 itibarıyla yürürlüğe girmesi beklenen devlete özel beyanlara ve coğrafyaya bağlı olacaktır.

Faydaları açıklamak için forma ekleyebileceğimiz bir satış belgesi olacak mı?

Evet, indirmeniz için bir ürün özeti mevcuttur.

Sigortalama Süreci

Bu değişikliklere karşı plan yapmak için neler yapabilirim? Müşteriler ve potansiyel müşterilerle yapacağım görüşmelerde bana yardımcı olacak kaynaklar sağlanacak mı?

Bu SSS'lari okuyup anlamanızın yanında Chubb tarafından verilecek tüm eğitim ve web seminerlerinden de faydalanmanızı öneririz. Yıl boyunca poliçe sahiplerinizle paylaşabileceğiniz tanıtım yazıları, web seminerleri ve videolar gibi çeşitli materyaller sunulacaktır. Daha fazla bilgi için meltem.yilmaz@chubb.com ile irtibata geçin.information.

Fiyatlandırma Süreci

Chubb'ın sunduğu sistemik teminatı ve fiyatlandırmayı etkileyen belirli sigortalama değerlendirmeleri var mı?

Evet. Chubb tarafından sunulan sistemik teminatı ve fiyatlandırmayı etkileyecek birkaç faktör vardır; bunların arasında, kuruluşun kritik bağımlılıkları, hizmet sağlayıcılarla yapılan sözleşmeye bağlı koruyucu önlemler, siber güvenlik koruması ve kontrolleri, olay müdahalesi/dayanıklılık planlaması ve testi yer almaktadır.

Yaygın Olay teminatının fiyatlandırma yapısında ne gibi bir değişiklik oldu?

Chubb tüm müşterilerine şeffaflık sağlamayı taahhüt eder ve sistemik teminat için ayrı fiyatlandırma, limit ve konservasyon seçenekleri sunacaktır.

Poliçe Formu

Chubb'ın yeni siber ürünlerinde hangi teminat hariç tutulmaktadır?

Yaygın Olaylara yönelik teminat hariç tutulmamaktadır. Sigortalanan olaylar için şeffaf bir şekilde kapasite sağlamak üzere yapılandırılmaktadır. Sigortalılar, Yaygın Olaylara yönelik teminat satın alma seçeneğine sahiptir ancak bu zorunlu değildir.

Sınırlı Etkiye Sahip Olay ve Yaygın Olay kavramları poliçenin neresinde açıklanmaktadır?

olarak sınıflandırılacağı ifade edilmektedir; bu tanımlar poliçede Bölüm II dahilinde ana hatlarıyla belirtilmiştir. Bu kavramlarda kullanılan diğer önemli tanımlar, diğerlerinin yanı sıra, Yaygın Tetikleyici ve Sınırlı Etkiye Sahip Grubu içerir.

Tüm Yaygın Olay türlerinde aynı limitleri, konservasyonları ve koasüransı sağlayan poliçeler için Yaygın Olayların dört alt kategorisi arasında bir ayrım yapmak önemli değildir. Ancak, farklı limitler, konservasyonlar veya koasürans varsa aşağıdaki Yaygın Olay alt kategori tanımları gözden geçirilmelidir:

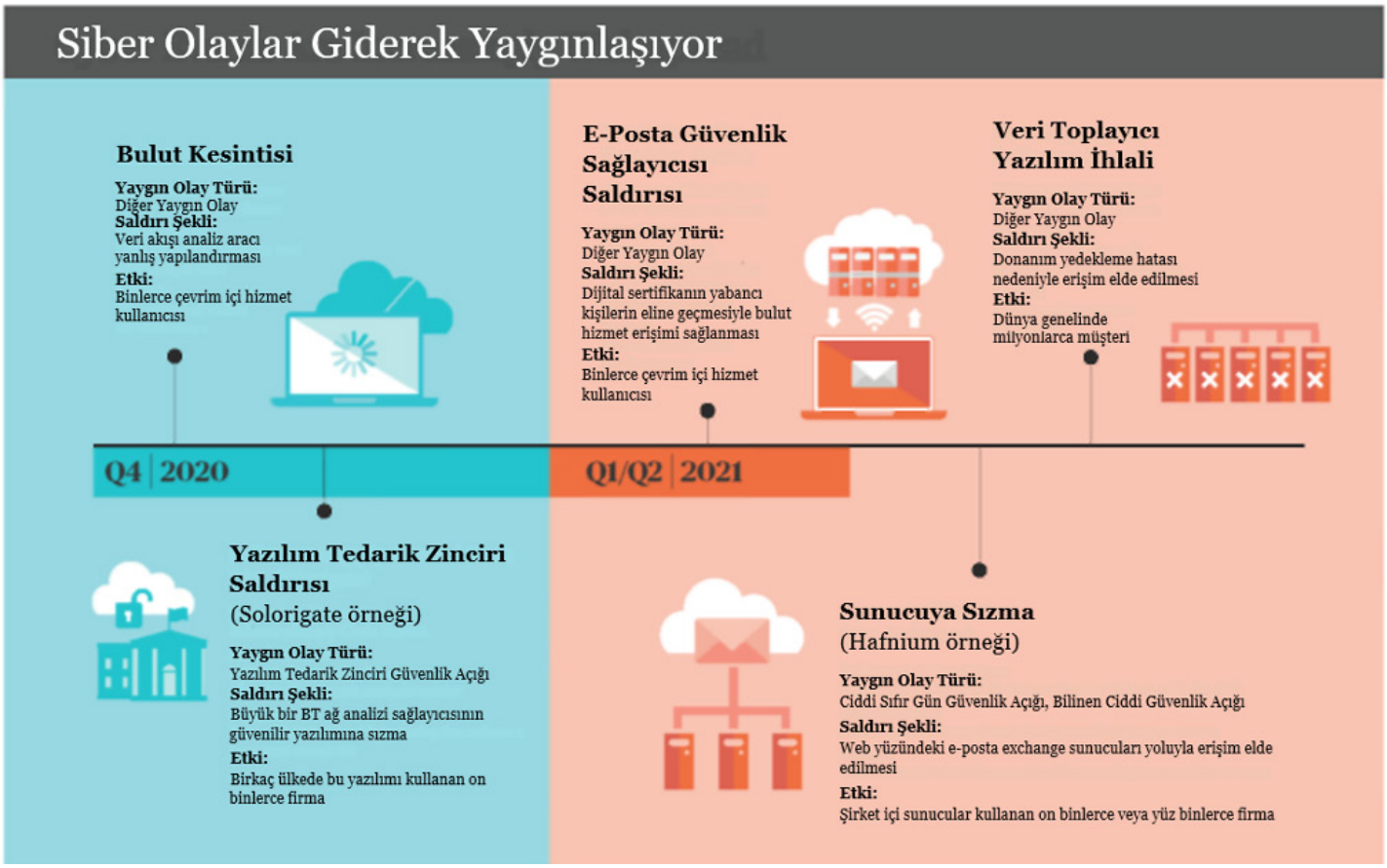
• Yaygın ve AğırBilinen Güvenlik Açığı

• Yaygın ve Ciddi Sıfır Gün Güvenlik Açığı

• Yaygın Yazılım Tedarik Zinciri Güvenlik Açığı

• Diğer Tüm Yaygın Olaylar

Poliçede "Fusion General Amendatory Endorsment" dahilinde "Bir Siber Olay Anındaki Görevler" ele alınır ve bir Siber Olay meydana gelmesi halinde poliçe sahibinin ve Chubb'ın nasıl bir iş birliği yapacağı ayrıntılı olarak açıklanır. Siber Olayın Sınırlı Etkiye Sahip Olay mı yoksa Yaygın Olay mı olduğunu belirleyecek yöntemler ve zamanlama konusundaki bilgiler bu kapsamdadır. Her zaman olduğu gibi poliçenin baştan sona okunması gerekir.



Yaygın Olaylara ilişkin geçmişte yaşanmış gerçek örnekler verebilir misiniz?

Son zamanlarda gerçekleşen yaygın olaylara ilişkin örnekler yukarıdaki grafikte verilmiştir.

Koasürans nasıl çalışır? Bir örnek verebilir misiniz?

Yaygın Olaylar, Fidye Yazılımı Olayları ve İhmal Edilen Yazılım Güvenlik Açıkları için uygulanabilir koasürans "kayıp azaltma" koasüransıdır ve bu da poliçe sahibi koasüransının sigorta limitlerini kullanmaması anlamına gelir. Bunun yerine, her bir kayba yönelik sorumluluk, sigortalı ile sigortacı arasında bölüştürülür ve ardından sigortacının payı ilgili risk için geçerli limite tabi olur.

Örneğin, poliçenin Yaygın bir Olay için 10 milyon ABD doları tutarındaki toplam poliçe limitinin %5'i oranında bir Alt Limiti varsa Sigortacının, ilgili Yaygın Olay Alt Limiti kapsamındaki Yaygın Olaya ilişkin kayıplara yönelik sorumluluğu en fazla 500.000 ABD doları olacaktır (yani, 10 milyon ABD dolarının %5'i).

Yaygın bir Olaya yönelik teminat %50 oranında koasüransa tabiyse 1 milyon ABD doları değerindeki bir kayıp olayı sigortacı ile sigortalı arasında yarı yarıya bölüştürülecektir ve sigortacı tüm mevcut 500.000 ABD doları tutarındaki Alt Limiti ödemiş olacağından Yaygın Olay Alt Limiti bunun ardından kullanılmış olacaktır.

Alternatif olarak, 500.000 ABD doları değerinde bir Yaygın Olay kaybı da yarı yarıya bölüştürülecek ancak sigortacı bu durumda yalnızca 250.000 ABD doları ödeyeceğinden gelecek olaylara yönelik Yaygın Olay Alt Limiti kapsamında geriye 250.000 ABD doları kalacaktır.

Son

1. National Institute of Standards and Technology Ulusal Güvenlik Açıkları Veri Tabanı. https://nvd.nist.gov/vuln/search adresinden alınmıştır
2. AV-TEST Institute (2021). www.av-test.org/en/statistics/malware/ adresinden alınmıştır
3. Federal Commission Warns Dangerously Insecure U.S. At Risk of 'Catastrophic' Cyber Attack (2020). www.forbes.com/sites/daveywinder/2020/03/14/ make-america-safe-again-federal-commission-warns-us-at-risk-of-catastrophic-cyber- at-tack/?sh=244402e34d27 adresinden alınmıştır
4. Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk (2021). www.insurancejournal.com/research/research/ransomware-and- aggregation-issues-call-for-new-approaches-to-cyber-risk/ adresinden alınmıştır
5. Ibid.
6. NIST Security Vulnerability Trends in 2020: An Analysis (2021). www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf adresinden alınmıştır

Chubb Hakkında

Chubb dünyanın halka açık en büyük mal ve kaza sigortası şirketidir. 54 ülke ve bölgede faaliyette olan Chubb, çeşitli müşteri gruplarına kurumsal ve bireysel mal ve kaza sigortası, ferdi kaza ve tamamlayıcı sağlık sigortası, reasürans ve hayat sigortası ürünleri sunmaktadır. Bir sigorta şirketi olarak riskleri içgörü ve disiplinle değerlendiriyor, üstleniyor ve yönetiyoruz. Hasar taleplerine adil bir şekilde hızlıca yanıt veriyor ve gerekli ödemeleri yapıyoruz. Şirketimiz aynı zamanda dünya genelinde kapsamlı ürün ve hizmet teklifleri, geniş dağıtım kapasitesi, olağanüstü mali gücü ve yerel operasyonları ile tanınmaktadır. Ana şirket Chubb Limited, New York Borsasına kotedir (NYSE: CB) ve S&P 500 endeksinde yer almaktadır. Zürih, New York, Londra, Paris ve diğer şehirlerde idari ofislere sahip olan Chubb dünya genelinde 31.000'den fazla kişi istihdam etmektedir.

Chubb'ın siber risk yönetimine ilişkin deneyimi ve uzmanlığı hakkında daha fazla bilgi almak meltem.yilmaz@chubb.com ile irtibata geçebilirsiniz

Chubb. Insured.℠