CHUBB®

Risk Hızının Yönetimi:

Yapay Zeka, Dava Süreçleri ve Dayanıklılık

2026 Siber Tazminat Talebi Raporu

Birinci Bölüm

Giriş: Ayrışma

Siber riskin doğası evrilmeye devam ederken, güvenlik açığı ve riske maruz kalma kapsamı genişliyor. Son rapora göre, yapay zeka destekli tespit sistemlerinin başarıyla entegre edilmesi ve dayanıklılığın artması sayesinde çok sayıda küresel pazarda 2025 yılında gerçekleşen siber vaka sayısının artması engellendi. ABD'de ise vakaların büyüklüğünde tarihi bir artış söz konusu. 2025 yılında, ortalama veri ihlali maliyeti **10,2 milyon $'ı aştı.** Bu rakam,4,4 milyon $ olan küresel ortalamanın iki katından fazla.

Sonuç olarak, herhangi bir şirketin —veya herhangi bir coğrafi pazarın— siber olaylara karşı korunmadaki başarısı; sürekli evrilen tehdit ortamını, veri edinme ve depolama faaliyetlerini düzenleyen yasal ve mevzuat çerçevelerini ve şirketin tedarik zinciri boyunca maruziyeti artıran iş ortakları arasındaki bağlantısallığı anlamasına bağlıdır.

Chubb'ın Siber Tazminat Talepleri raporunun bu sürümü, Chubb'ın 2025 Aralık tarihine kadarki geçmiş tazminat talebi verilerini inceleyerek tazminat talebi sıklığı ve büyüklüğü trendleri ile bu trendleri besleyen etkenler hakkında içgörü oluşturmak; bu sayede de işletmelerin karmaşık siber risk ortamında ilerlemelerine ve mali ve operasyonel dayanıklılık oluşturmalarına yardımcı olmaktır.

Kaynak: *IBM Cost of Data Breach Report 2025*

İkinci Bölüm

Küresel Tazminat Talebi Trendleri

Tüm pazarlardaki siber tazminat talepleri, teknolojideki ve yasal ortamdaki değişikliklerin yanı sıra tedarik zincirlerinin birbirine bağımlılığından güç aldı. Üç trend dikkat çekiyor.

01

Yapay zeka, riski hızlandırıyor.

Siber vakaların daha hızlı ve daha ayrıntılı tespit edilmesine olanak tanıyan yapay zeka teknolojisi, vaka hızını da temelden değiştirdi. Kötü amaçlı yazılımlarda özerk ve otonom yapay zeka kullanan kötü niyetli kişiler, artık yalnızca birkaç dakika içinde çok sayıda sisteme saldırabiliyor ve bu da insan müdahalesini imkansız hale getiriyor. Kötü niyetli kişilerin, Geniş Dil Modelleri (Large Language Model veya LLM) gibi gelişmiş yapay zeka teknolojilerini kullanma hızları neredeyse günlük müşterilerin yapay zeka kullanma hızıyla aynı hızda artıyor.

02

"Önce dava et" refleksi.

Siber vaka, artık çözülmesi gereken bir teknik hata değil; sıklıkla vakanın ardından kısa süre içinde dava açılıyor. Son 30 yılda, gizlilik ve veri koruma yasaları olağanüstü bir hızla yürürlüğe girmiş; bu durum, uyumluluk süreçlerinin karmaşıklığını ve gizlilikle ilgili davaların sıklığını artırmıştır. İhlal ile ilk toplu dava başvurusu arasındaki süre belirgin biçimde kısalmıştır; dava çoğu zaman günler içinde açılmakta ve iddialar, kuruluşun büyüklüğünden ya da yetersiz olduğu düşünülen kontrollerden bağımsız olarak farklılık gösterebilmektedir.

03

Sistemik birbirine bağımlılık.

Birkaç yıl öncesine kadar risk yöneticileri, kendi siber aksaklıklarının müşterilerini ve tedarikçilerini etkilemesini önlemeye öncelikli olarak odaklanıyordu. Günümüzde, kuruluşun kendi tedarik zincirinin siber olayların sıklığı ve şiddeti üzerindeki önemli etkisine ilişkin farkındalıklar yaygınlaştı.

Dünya Ekonomi Forumu'na göre, siber konusunda en büyük güçlüğün üçüncü taraf ve tedarik zinciri güvenlik açığı olduğunu dile getiren büyük şirket oranı 2025'te %54 iken günümüzde %65'e ulaşmıştır.

Küresel Otomobil Üreticisi Siber Vakası

Daha ayrıntılı olarak ilerleyen bölümlerde açıklandığı üzere, Ağustos 2025'te yaşanan Global Car Manufacturer siber olayı gibi vakalar, tedarik zincirinin herhangi bir halkasında meydana gelen bir siber olayın ağır ekonomik ve operasyonel etkilerini ortaya koymuştur. Vaka, tüm İngiltere ekonomisi üzerinden bir şok dalgası oluşturmuş ve bir anda geniş çaplı etkiye yol açmıştır. Otomobil üreticisi, üretimin durması nedeniyle yaşadığı devasa finansal kayıplara ek olarak vakayla ilgili çok sayıda toplu davayla da karşı karşıyadır.

Üçüncü Bölüm

Siber Olayların Sıklığı ve Şiddeti

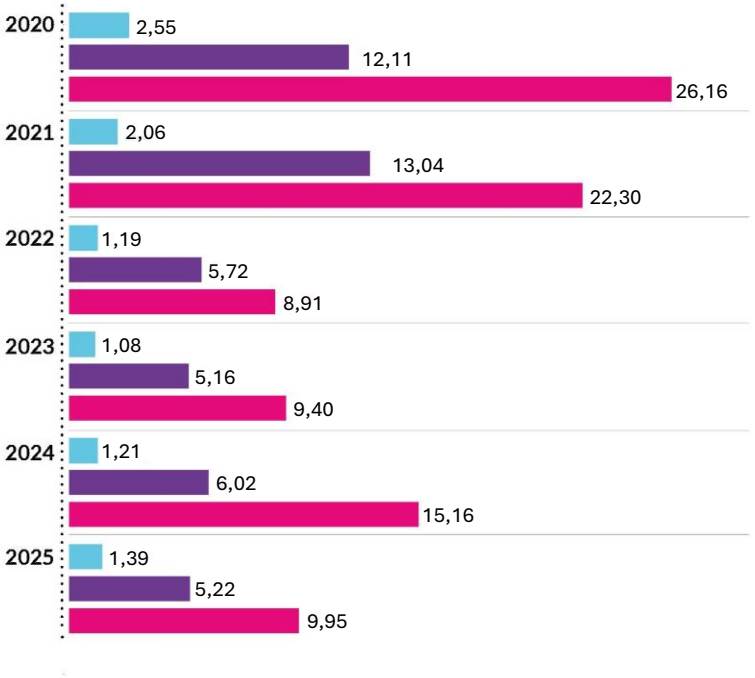
Frekans, poliçe başına düşen hasar sayısını; şiddet ise hasar başına ortalama maliyeti ifade eder. Bu iki unsur, sigorta hasar maliyetlerinin temel bileşenleri olup sigorta primlerindeki değişimlerin başlıca belirleyicileridir. Sigorta, doğası gereği tahsil edilen primin gerçek hasar maliyetlerinin gerisinde kaldığı bir iş kolu olduğundan, sıklık ve şiddetteki son dönem tarihsel eğilimler, gelecek yıl uygulanacak oranlar için önemli bir öncü gösterge niteliğindedir.

Yandaki tablolar, son altı yılda ABD siber ortamında karışık bir sıklık ve büyüklük eğilimi göstermektedir.

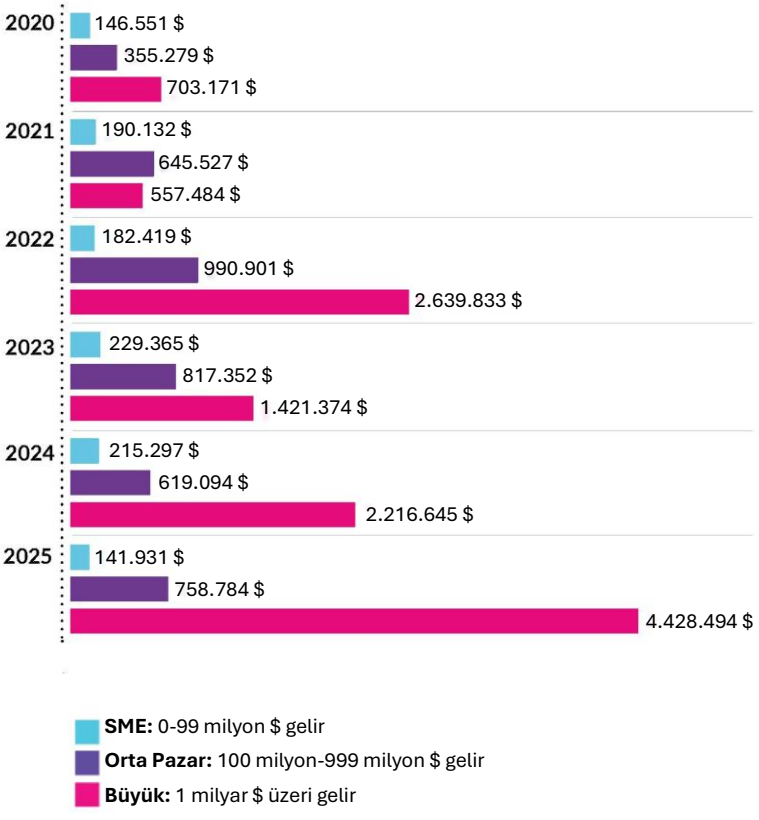
Müşterilerin güvenlik profillerindeki ve dayanıklılık becerilerindeki iyileşmeler, 2020 ile 2022 yılları arasında her büyüklükten işletmenin karşılaştığı tazminat talebi sıklığındaki ciddi azalmaya yansımıştır. Veri aynı zamanda, 2022 yılından beri küçük ve orta büyüklükteki işletmelerde (SME) ve büyük risk topluluklarında genel bir artış göstermekle birlikte orta pazar aynı dönemde daha istikrarlı kalmıştır.

Büyüklük artmasına karşın limit kullanımı 2021'den beri düşmektedir. Büyüklük SME segmentinde sabit kalsa da orta pazarda önemli düzeyde, büyük hesap segmentinde ise daha da şiddetli bir artış söz konusudur. Bu artışa neden olan çok sayıda etken mevcuttur. İş kesintisi masraflarının artması, gerek veri ihlali gerekse mahremiyetle ilgili açılan dava maliyetlerinin artması bu etkenler arasında yer almaktadır.

100 Poliçe Başına Siber Tazminat Talebi Sıklığı (ABD)

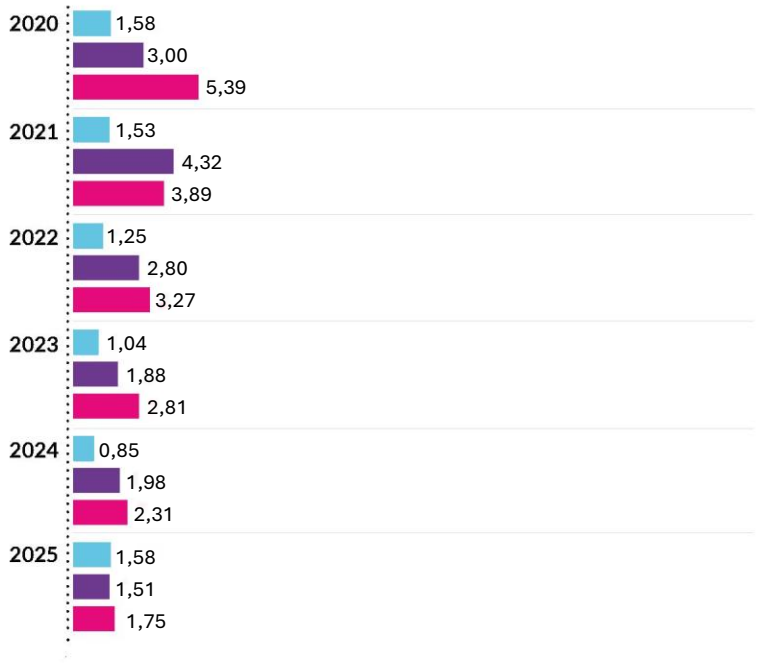


Siber Tazminat Talebi Ortalama Büyüklüğü (ABD)

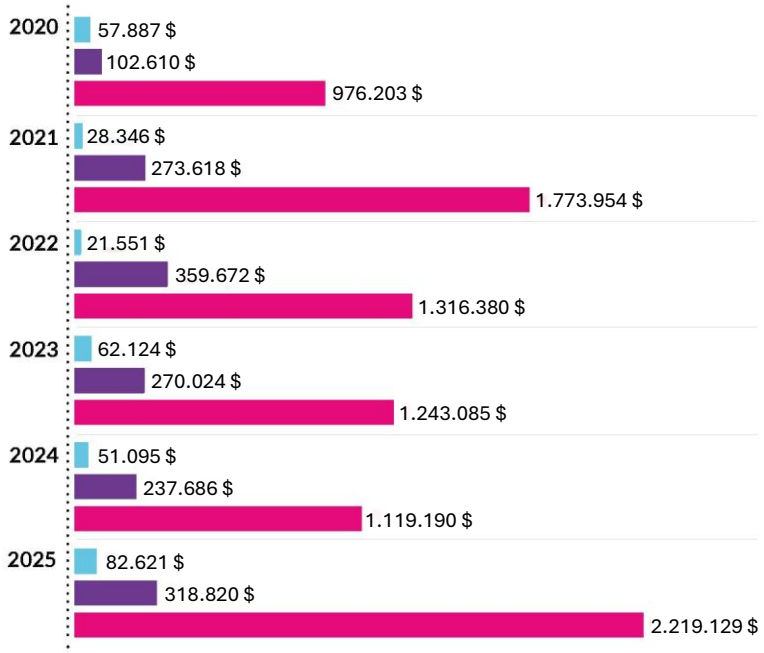


SME: 0-99 milyon $ gelir
Orta Pazar: 100 milyon-999 milyon $ gelir
Büyük: 1 milyar $ üzeri gelir

100 Poliçe Başına Siber Tazminat Talebi Sıklığı (Avrupa + BK)



Siber Tazminat Talebi Ortalama Büyüklüğü (Avrupa + BK)



SME: 0-99 milyon $ gelir
Orta Pazar: 100 milyon-999 milyon $ gelir
Büyük: 1 milyar $ üzeri gelir

Avrupa ve BK'da gözlenen eğilimler ABD ile kıyaslandığında zaman zaman benzerlikler zaman zamansa farklılıklar göstermektedir.

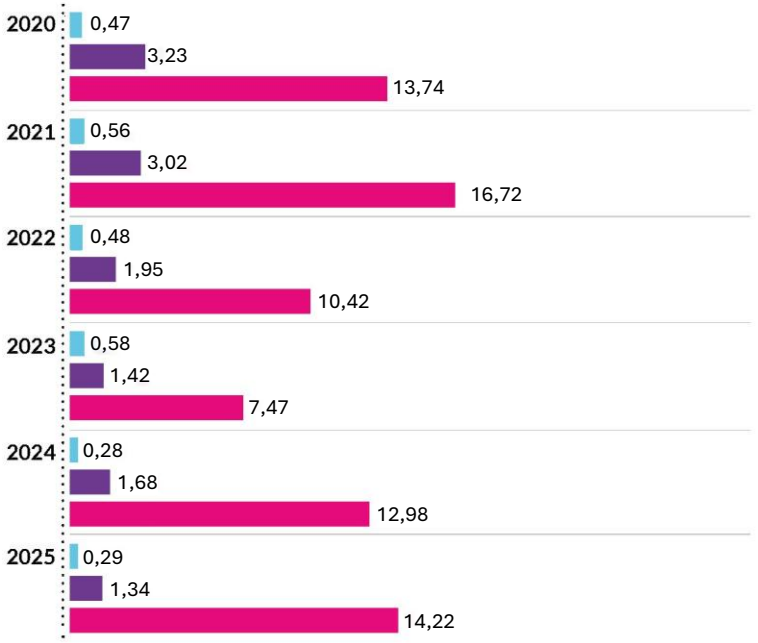
KOBİ grubunda sıklık düzeyleri benzerdir ancak orta pazarda ve büyük hesap segmentlerinde çok daha düşüktür. Bu, ABD, Avrupa ve BK'da saldırıya uğrama eğilimi ile uygulanan genel güvenlik profili ve kontrollerinin KOBİ'ler çapında benzer olduğuna işaret etmektedir. Diğer yandan, Avrupa ve BK'daki orta ve büyük şirket segmentlerindeki maruziyet ABD'ye kıyasla net bir şekilde düşüktür. Bu fark, büyük oranda üçüncü taraf davalara ilişkin tazminat talebi olmamasından kaynaklanmaktadır.

Büyüklük, tüm Avrupa ve BK gruplarında düşüktür. Bu da büyük oranda, veri ihlali içeren veya içermeyen mahremiyet davalarından doğan kayda değer üçüncü taraf dava maliyeti bulunmamasından kaynaklanmaktadır. Büyüklük tüm gruplarda net bir biçimde artış gösterse de ABD'ye nazaran daha istikrarlıdır.

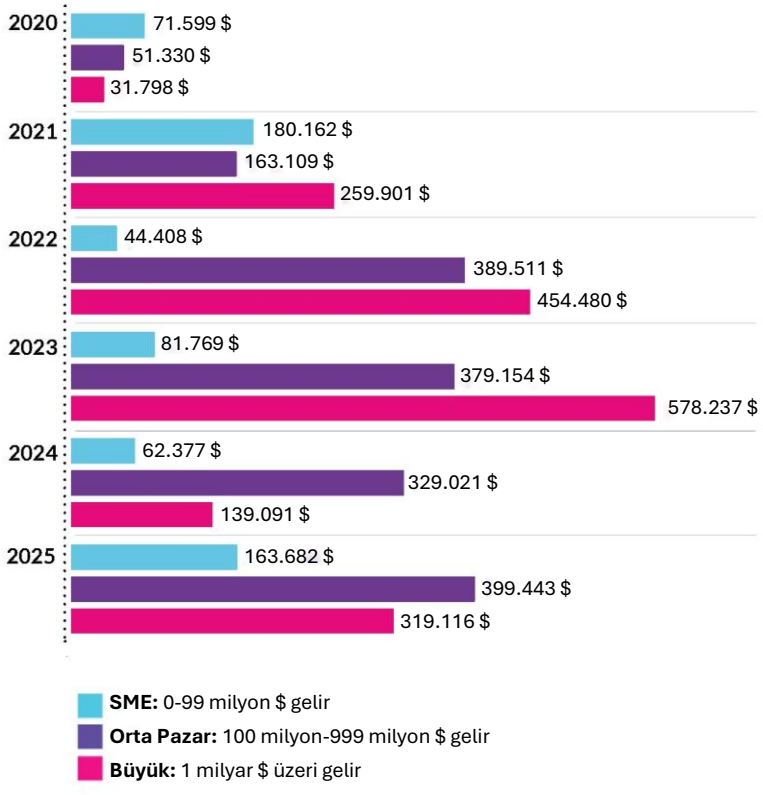
Avustralya ve Yeni Zelanda'da, sıklık, şiddet ve genel eğilimler dünyanın diğer bölgelerine kıyasla farklılık gösterse de, genel olarak aynı yönde ilerlemektedir.

2021 sonrasında olayların sıklığı belirgin biçimde azalırken, şiddeti genel olarak artış göstermiştir. KOBİ'lerde sıklık, dünyanın diğer bölgelerindeki seviyelerin çok küçük bir kısmı düzeyindeyken, şiddet yaklaşık olarak aynı seviyededir. Orta ölçekli piyasalarda sıklık, Avrupa ve Birleşik Krallık ile paralel seyretmekte ve ABD'ye kıyasla çok daha düşük kalmaktadır; bu durum, siber veri ihlali ve veri dışı gizlilik davaları açısından görece daha ılımlı olan hukuki ortamı yansıtmaktadır. Dikkat çekici bir diğer husus, orta ölçekli piyasa ve büyük şirket segmentlerinde şiddet seviyelerinin daha düşük olması ve zaman içinde daha sınırlı artış göstermesidir.

100 Poliçe Başına Siber Tazminat Talebi Sıklığı (Avustralya ve Yeni Zelanda)



Siber Tazminat Talebi Ortalama Büyüklüğü (Avustralya ve Yeni Zelanda)



Dördüncü Bölüm

Yapay Zeka Savaşları: Saldırı ve Savunma

Yapay zekanın küresel ölçekte giderek daha fazla benimsenmesi ve gelişmesi, teknolojinin giderek daha sofistike kötü niyetli kullanımlarının yanı sıra, faydalı tespit ve iyileştirme araçlarının da ortaya çıkmasını beraberinde getirmiştir.

Chubb'ın siber sigorta ürünleri yapay zeka da dahil olmak için her tür siber olayı içerir. Pazardaki alternatiflerin kapsamları — örneğin yapay zekâ klozları, alt limitler veya daha dar kapsamlı teminatlar — sigortalılar ve brokerlar tarafından dikkatle değerlendirilmelidir.

Örneğin Kasım ayında, yapay zekâ aracı Claude'un arkasındaki şirket olan Anthropic, yapay zekânın ajan benzeri yeteneklerini benzeri görülmemiş ölçüde kullanan suçluların yürüttüğü "son derece sofistike bir casusluk kampanyasının" kurbanı olduğunu bildirmiştir.

Yapay zeka, yalnızca tavsiye sağlayan bir unsur olarak değil siber saldırıyı yapan unsur olarak kullanılmıştır. Büyük teknoloji şirketleri, finans kuruluşları ve kamu kurumları başta olmak üzere çeşitli kuruluşları hedef alan bu saldırı, Anthropic'in değerlendirmesine göre, "önemli ölçüde insan müdahalesi olmaksızın gerçekleştirilen ilk belgelenmiş büyük ölçekli siber saldırı" olmuştur.

Ajan tabanlı yapay zekânın ve otonom kötü amaçlı yazılımların kötü niyetli kullanımına ilişkin diğer gelişmeler şunlardır:

İmza tabanlı tespit önlemlerini atlatmak için çalışırken kendini yeniden yazan kodlar.

Kurumsal ağların tamamını haritalandıran ve güvenlik açıklarını anında tespit ettikten sonra hedefli saldırılar başlatan otonom keşif sürüleri — "dijital çekirgeler" —.

Mali işler direktörleri veya diğer yöneticilerin seslerini ustalıkla taklit ederek çalışanları yetkisiz para transferleri yapmaya kandırmak üzere hiper-gerçekçi deepfake'leri geliştiren ve optimize eden yapay zekâ.

Buna ek olarak, bir çalışanın Kişisel Olarak Tanımlanabilir Bilgileri (PII) yanlışlıkla herkese açık bir LLM'e yüklemesi ve bunun bir siber olaya yol açması gibi, daha az karmaşık yapay zekâ kaynaklı olaylar da devam etmektedir.

Güvenlik önlemleri tarafında ise işletmeler ve kuruluşlar, bu tehditlere yanıt vermek ve risklerini azaltmak için kanıtlanmış, yapay zekâ odaklı risk azaltma araçlarını devreye alabilir.

Bunlar:

Yapay Zeka Önceliklendirmeli Güvenlik önlemleri: Gerçek zamanlı tehdit tespiti için yapay zekâ destekli güvenlik operasyonlarının (AISO) benimsenmesi.

Yapay Zeka Yönetimi: Tüm yapay zeka sistemleri için sıkı bir envanterini tutmak ve üçüncü taraf veri işleme uygulamalarını denetlemek.

Gelişmiş eğitim: Çalışanları, gelişmiş kimlik avı ve derin sahte montajlar gibi yapay zeka temelli güvenlik riskleri konusunda eğitmek.

Beşinci Bölüm

Sosyal Mühendislik Dolandırıcılığının Etkisi

Sosyal mühendislik dolandırıcılığı davaları, özellikle küçük ve orta ölçekli işletmeler için ağır sonuçlar doğurabilir. Finansal kayıplar, operasyonel aksaklıklar ve itibar kaybı riski, etkili müdahale ve toparlanma stratejilerine duyulan kritik ihtiyacı ortaya koymaktadır.

Sosyal Mühendislik Dolandırıcılığı Kaynaklı Siber Olay

Olay: Uzun süredir çalışılan bir makine tedarikçisinin temsilcisinden gelmiş gibi görünen bir e-postaya güvenen yeni bir çalışan, e-postayı tedarikçinin ofisini arayarak doğrulamaya çalışmadan, satıcıya yapılacak ödemenin banka bilgilerini yeni bir banka hesabı ile değiştirmiştir.

Etki: Şirket, daha sonra tedarikçinin gerçek çalışanı ödeme için takip yaptığında, çalışanın sosyal mühendislik dolandırıcılığının kurbanı olduğunu fark eder; bu sırada e-postanın sahte olduğu ve ödemenin bir sahtekâra yapıldığı anlaşılır.

100.000 $

Çözüm: 100.000 $'dan fazla kayıp.
Banka veya tedarikçiden tahsilat yapılamaz.

Sonuç: Siber poliçe, siber suç teminatı içeren bir klozla birlikte, sigorta ettirene geri kazanılamayan zararlarını tazmin eder.

Altıncı Bölüm

Gizlilik Sınırı ve İlk Başvuru Olarak Dava Eğilimi

Siber olaylar giderek daha fazla hukuki vakaya dönüşürken, şirketler özellikle dinleme ve dijital izleme teknolojilerine ilişkin yeni sorumluluk teorilerinin ortaya çıkardığı hukuki zorluklarla karşı karşıya kalmaktadır.

Yasal yükümlülüğü etkileyen ana etkenler:

"Önce Dava Et" Refleksi: ABD'de, davacılar onlarca yıllık telekulak kanunlarını (örneğin **Kaliforniya Gizlilik İhlali Kanunu**) ve video mahremiyet yasaları (örneğin **Video Koruma Gizlilik Yasası**) kullanarak piksel takibi dahil olmak üzere standart web teknolojilerini hedef almaktadır.

Veri ve mahremiyet yasaları: BK ve Avrupa'da evrilen gizlilik düzenlemeleri **Genel Veri Koruma Düzenlemesi (GDPR)** ve **BK Veri Koruma Yasası** temel alınarak oluşturulan **Veri (Kullanım ve Erişim) Yasası 2025 (DUAA)**, takip pikselleri gibi standart web teknolojilerinin kullanımı da dâhil olmak üzere, kişisel verilerin işlenmesi konusunda şirketler için karmaşık yükümlülükler ortaya çıkarmıştır.

Toplu Tahkim: ABD'deki şirketler, açılan her dosya için ciddi idari ücretler ödemek zorunda kalmaktadır. Örneğin 10.000 davacının yer aldığı bir davada, iadesi olmayan bu ücretler, daha davanın esası dinlenmeden 10 milyon $'ı aşan bir meblağa ulaşabilir.

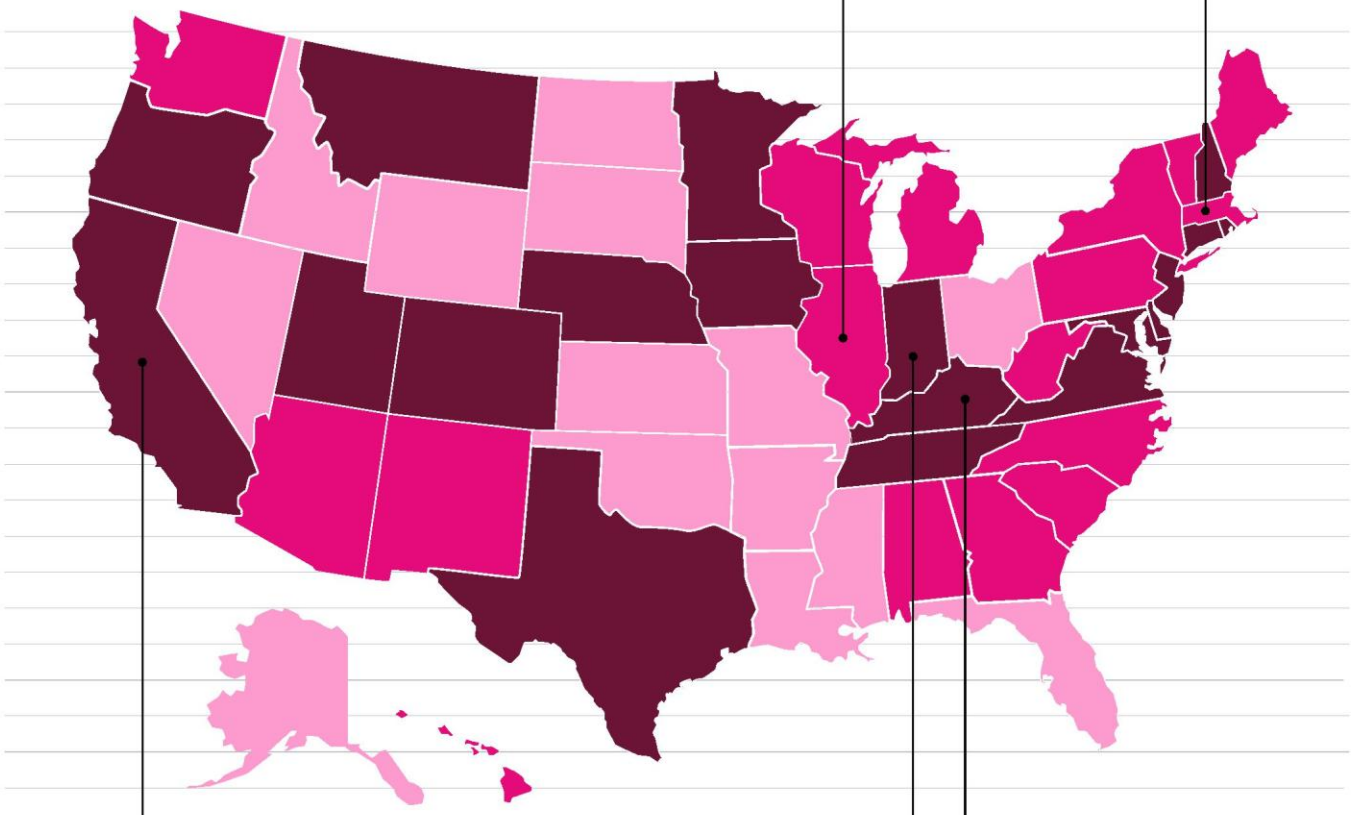
Veri Baskılama: Saldırganlar, verileri yalnızca şifrelemek yerine kasıtlı olarak silmeye veya sızdırmaya yönelmekte; bu da kalıcı bir "kontrol kaybı" yaratarak davalarda riskleri artırabilmektedir.

ABD ve AB'de giderek artan gizlilik mevzuatı, kişisel verileri saklayan ve/veya aktaran şirketler için karmaşık ve çok katmanlı yükümlülükler getirmektedir. Bunlar arasında, profilleme veya otomatik karar verme süreçlerinden çıkma hakkı, yapay zekâ destekli işleme faaliyetlerine ilişkin açıklama yükümlülükleri ve yüksek riskli kullanım alanları için zorunlu risk değerlendirmeleri yer almaktadır.

Amerika Birleşik Devletleri

Gizlilik Mevzuatı Takibi

Federal bir mevzuat bulunmamaktadır ve eyaletlere göre değişen düzenlemeler söz konusudur.



Kaynak: *ABD Federal Mahremiyet Mevzuatı Takibi*

ABD ile veya ABD içinde ticaret yaparken düzenlemelerin eyalete göre değiştiğini göz önünde bulundurmak BK ve Avrupa'daki şirketler için önemlidir. Daha fazla bilgi almak için **Chubb Siber Sigorta** sayfasını ziyaret edin.

Yedinci Bölüm

Hassas Verilerin Korunması

Gizlilik vakaları, siber davaların gerek sıklığı gerekse büyüklüğü açısından artan bir kaynaktır. Gelişen düzenlemeler ve büyük ölçekli davaların artışıyla birlikte, gizlilik riskini yönetmek daha karmaşık ve maliyetli hale gelmiştir. Her kuruluş, sürekli değişen tehdit ortamında verileri koruma konusunda kendine özgü zorluklarla karşılaşabilir.

Tüketici gizliliği risklerini yönetmek ve düzenleyici uyumu sağlamak büyük önem taşımaktadır. Sigortalılarımızı desteklemek amacıyla Chubb, sigortalıların gizlilik risklerini değerlendirerek ve proaktif biçimde yöneterek, hassas verileri koruyarak ve uyumu sürdürerek kuruluşlarını güvence altına almalarına olanak tanıyan gizlilik risk yönetimi platformlarıyla iş birliği yapmıştır.

Orta Pazar Mahremiyet Vakası

Olay: Sigortalı, çerezler ve pikseller dâhil olmak üzere izleme teknolojileri kullanan abonelik bazlı bir web sitesi ve mobil uygulama işletmektedir. Piksel, web sitesi kullanıcısının kullanıcı kimliği dâhil olmak üzere belirli verileri takip eder ve bu verileri üçüncü taraflara iletir.

Etki: Birden fazla hukuk bürosu, piksel kullanımının, rıza olmaksızın iletişimlerin dinlenmesini yasaklayan California Invasion of Privacy Act'i ihlal ettiğini ileri sürerek binlerce tahkim öncesi talep göndermiştir.

40 milyon $ üzeri

Sorun: Sigortalının gizlilik politikası, tüm uyuşmazlıkların tahkim yoluyla çözülmesini zorunlu kılıyordu. Ancak tahkim kurumunun kuralları, sigortalının daha en başta birkaç milyon ABD doları tutarında başvuru ücretini ödemesini gerektirecekti. Dolayısıyla, talepler tahkime taşınsaydı, bu durum potansiyel olarak yasal tazminat hükmü ile birlikte 40 milyon ABD dolarını aşan tahkim ücretlerine yol açabilirdi.

Çözüm: Chubb, gizlilik davalarında deneyimli bir avukat ve avukatlık bürolarıyla anlaşarak uzlaşmazlığın arabuluculukla çözülmesini sağlamıştır.

6,5 milyon $

Sonuç: Küresel çapta çok sayıda tazminat talebi, 6,5 milyon $ gibi bir meblağ ile çözülmüştür.

Sekizinci Bölüm

Fidye Yazılımının Küçük Orta Ölçekli Girişimler Üzerindeki Etkisi

Fidye yazılımı saldırıları, küçük ve orta ölçekli girişimler (KOBİ) için ciddi bir risk oluşturmaya devam etmekte ve sıkça karmaşık ve maliyetli veri ihlalleriyle sonuçlanmaktadır. İlk şifreleme girişimleri engellense bile, hassas bilgilerin dışarı sızdırılması kapsamlı bildirim yükümlülüklerini ve düzeltici faaliyetleri tetikleyebilir.

Chubb, fidye yazılımı talepleri konusunda önemli bir deneyime sahiptir ve sigortalılarımızın fidye yazılımı olaylarına etkili biçimde yanıt verip süreci sorunsuz yönetmelerine yardımcı olmak için hukuk, BT adli bilişim, halkla ilişkiler ve diğer uzmanlık alanlarında yüksek itibara sahip hizmetler sunar; bu kapsamda hasar gören sistemlerin onarılması veya yenilenmesi, kesinti süresinin en aza indirilmesi ve iş sürekliliğine dönüş desteklenir.

KOBİ Fidye Yazılımı Vakası

Olay: Bir siber saldırı grubunun sigortalının bilgisayarını şifreleme girişimleri, sigortalının uç nokta algılama ve müdahale aracı sayesinde büyük ölçüde engellenmiştir. Ancak, saldırgan, 4 milyonu aşkın kişinin sağlık bilgilerini ve kimlik numaralarını dışarı sızdırmayı başarmıştır.

Etki: Sigortalının, yürürlükteki kanun ve düzenlemelerle zorunlu kılınan bildirim yükümlülüklerine uyum sağlamak için, tam olarak hangi verilerin ve kişisel sağlık bilgilerinin ihlal edildiğini hızla tespit etmesi gerekiyordu.

Sorun: Veri ihlalinin boyutunu anlamak, etkilenen kişilere zamanında bildirimde bulunulmasını sağlamak ve potansiyel olarak istismar edilen yamalanmamış güvenlik açıklarının mümkün olan en kısa sürede giderilmesini temin etmek.

4 milyon $

Çözüm: Bu olaya yanıt verilmesi sürecinde sigortalıya destek olmak üzere derhal hukuk müşavirleri, adli bilişim ekibi ve veri madenciliği ekibi görevlendirilmiştir. Etkilenen verilerin ayrıntılı incelemesinin ardından, 4 milyon kişi ve çok sayıda düzenleyici kurum bu olay hakkında bilgilendirilmiştir. Chubb Risk Advisor ekibi de, müşterinin yamalanmamış güvenlik açıklarını gidermesine yardımcı olmak üzere sürece dâhil edilmiştir.

4,7 milyon $

Sonuç: Sigortalıya geri ödenen toplam tutar 4,7 milyon ABD doları olup, bunun 2,4 milyon ABD doları bildirim maliyetlerini ve 1,2 milyon ABD doları mağdurlar için kredi izleme maliyetlerini kapsamaktadır. Sigortalıya ayrıca yamalanmamış güvenlik açıkları hakkında bildirim yapılmış ve bu açıkların giderilmesi konusunda destek sağlanmıştır.

Dokuzuncu Bölüm

Sınır Tanımayan Fidye Yazılımları

Fidye yazılımı saldırıları, dünyanın her yerinde organizasyonlar için ciddi riskler oluşturmaya devam etmektedir. Saldırganlar hassas verileri dışarı sızdırıp veriyi ifşa ettiklerinde, gelişmiş siber güvenlik önlemlerine sahip kurumlar bile geniş çaplı kesintiyle karşı karşıya kalır. Sonuçlar çoğu zaman farklı yargı alanlarına uzanarak düzenleyici incelemeyi, hukuki yükümlülükleri ve operasyonel zorlukları beraberinde getirmektedir.

Avrupa'da meydana gelen bu vakadan görüleceği üzere fidye yazılımı coğrafi sınır tanımaz.

Küresel Fidye Yazılımı Vakası

Olay: O dönemde kimliği bilinmeyen bir tehdit aktörü grubunun gerçekleştirdiği fidye yazılımı saldırısı, küresel bir akademik kurumu ve yayın kolunu hedef almıştır. 575.000'den fazla hassas belge dışarı sızdırıldı ve ardından grubun ifşa sitesinde yayınlandı.

Etki: Faaliyetler küresel çapta durdu. Yazar gelirleri, devlet araştırmaları ve gelecekteki sınav soruları dâhil olmak üzere hassas veriler, 40'tan fazla ülkede ifşa edilmiştir. İyileşme süreci, karmaşık BT bağımlılıklarının bulunduğu bölgelerde özellikle zorlu olmuştur.

Sorun: Düzenlemeye ilişkin riskleri belirlemek amacıyla akademik kurum, sızdırılan 575.000 belgenin tamamını değerlendirmek zorunda kalmıştır. 40 farklı yargı alanında hukuki danışmanlık alınması gerekmiş, bu durum karmaşıklığı önemli ölçüde artırmış ve küresel uyum gerekliliklerini karşılama baskısını yükseltmiştir.

Çözüm: Chubb, hukuki ve adli bilişim uzmanlarını görevlendirmiş; gelişmiş veri madenciliği sayesinde yüksek riskli içerikler tespit edilerek hızlı ve büyük ölçüde otomatik bir inceleme süreci mümkün kılınmıştır. Kıtalar genelinde koordine edilen hukuki katkı, düzenleyici bildirimlerin doğru ve zamanında yapılmasını sağlamıştır.

14,2 milyon $

Sonuç: Toplam hasar14,2 milyon ABD doları olup, buna siber olay müdahale giderleri ve iş kesintisi kaybı dâhildir. Hızlı aksiyon ve koordine edilen hukuki destek sayesinde akademik kurum, para cezaları, düzenleyici soruşturmalar veya yaptırımlardan kurtuldu. İhlalin büyüklüğüne rağmen itibar kaybı ve düzenlemeye ilişkin etkiler başarıyla sınırlandırıldı.

Onuncu Bölüm

Yaygın Olaylar: Birbirine Bağımlılığın Dalga Dalga Yayılan Maliyetleri

Hiçbir işletme izole bir şekilde faaliyet göstermez: iş ortakları vardır, tedarikçileri vardır, müşterileri vardır. 2025 yılında gerçekleşen iki kayda değer siber saldırı, bir fidye yazılımı saldırısında oluşan hasarın şirketin tedarik zincirindeki yukarı ve aşağı yönde birden çok işletmeyi nasıl etkileyebileceğini gözler önüne sermiştir. Chubb 2022 yılına dikkat çekerken, bu tür olayların şiddeti artık siber ekosistemin genelinde çok daha belirgin biçimde ortaya çıkmaktadır.

Birleşik Krallık – Ağustos 2025

Küresel Otomobil Üreticisi

Ağustos 2025'in sonlarında Global Car Manufacturer'a yönelik saldırı, Britanya tarihindeki en yıkıcı siber saldırı olayıdır. Olay hakkındaki ayrıntılar, tüm şirketler için önemli dersler içeren eğitici bir vaka haline geldi.

Vaka

"Scattered Lapsus Hunters" grubuna atfedilen saldırı, ihlali kontrol altına almak amacıyla küresel BT ağlarının devre dışı bırakılmasını zorunlu kılmıştır.

Faaliyetlere Etkisi

UK, Slovakya, Brezilya ve Çin'de üretim beş hafta boyunca durdu. Felç olan sistemler arasında üretim hattı kontrolleri, CAD/PLM tasarım ekipmanı ve bayi sipariş platformları da vardı.

Güvenlik ve Yasal Sonuçlar:

Hackerlar, maaş verilerini ve 7,4 milyon kişinin müşteri kayıtlarını dışarı sızdırarak kapsamlı bir dava sürecine yol açtı.

Sistemik Finansal Sonuçlar

1,9 milyar £

Ekonomik

UK ekonomisi tahminen 1,9 milyar £ (2,5 milyar $) kayba uğradı ve bu durum, 2025 yılının 3. çeyreğinde yaşanan GSYIH yavaşlamasının etkenlerinden biriydi.

1,2 milyar £

Tedarik Zinciri Etkisi

UK'ta 5000'in üzerinde organizasyon bu durumdan etkilendi. Zinciri stabilize etmek için devlet 1,2 milyar £ acil durum kredisi açarak duruma müdahale etti.

485 milyon £

Şirket Kaybı

Küresel Otomobil Üreticisi, vergi öncesi 485 milyon £ zarar açıkladı ve önceki yıl elde edilen 398 milyon £ kâr kaybedilmiş oldu.

Amerika Birleşik Devletleri – Şubat 2025

Oracle Health Veri İhlali

2025'in başlarında Oracle Health (eski adıyla Cerner), analistlerin ABD sağlık sektörünün tarihindeki en büyük ihlallerden biri olarak değerlendirdiği **büyük bir veri ihlali** yaşamıştır.

Vaka

Saldırganlar, çaldıkları kimlik bilgilerini kullanarak henüz Oracle Cloud'a taşınmayan eski Cerner veri mitigasyonu sunucularına eriştiler.

Kilit Açık

İhlal, bazı bölümleri 2017 yılından beri kullanılmayan eski bir ortamı hedef almıştı. Ana hedef, "unutulmuş" verilerdi.

Etki

Saldırı, yaklaşık 80 hastaneye ait kayıtları ele geçirerek hastaların Sosyal Güvenlik numaralarını ve tanı ile tedavi görüntüleri dâhil olmak üzere tıbbi geçmişlerini ifşa etmiştir.

Şantaj Faktörü

Andrew takma adlı bir saldırgan, çalınan dosyaları ifşa etmemek için kripto para cinsinden milyonlar talep etti.

2025'te yaşanan bu ve benzeri olaylar — aralarında kasıtlı kötü niyetten ziyade hata veya kazalardan kaynaklanan birçok vaka da bulunmakta olup (örneğin Ekim ayındaki Amazon Web Services kesintisi) — mevcut en sıkı siber risk azaltma önlemlerinin belirlenmesi ve uygulanması gerekliliğini ortaya koymaktadır.

Bu senaryolar küçük işletmelere uzak görünebilir; ancak Chubb'ın deneyimi, bunun gerçeği yansıtmadığını göstermektedir.

KOBİ Tedarikçi Olayı

Olay: Sigortalı perakendeci, günlük operasyonlar için gerekli yazılımı sağlamak üzere üçüncü taraf bir teknoloji sağlayıcısıyla sözleşme yapmıştır. Teknoloji sağlayıcısı bir fidye yazılımı saldırısının hedefi olduğunda, tüm sistemleri çevrimdışı kalmıştır.

Etki: Yazılımı kullanamayan sigortalı, belirli ürünlerin satışını gerçekleştirememiş, stok siparişi verememiş veya müşteri randevularını planlayamamıştır.

Çözüm: Chubb, ortaya çıkan koşullu iş kesintisi kaybının hesaplanmasında sigortalıya yardımcı olmak üzere bir adli muhasebeci görevlendirmiştir. Sigortalının olay müdahale planı doğrultusundaki hazırlığı ve Chubb hasar süreciyle entegrasyonu, büyük ölçüde sigortalının kontrolü dışında gelişen bu olayın yönetilmesine yardımcı olmuştur.

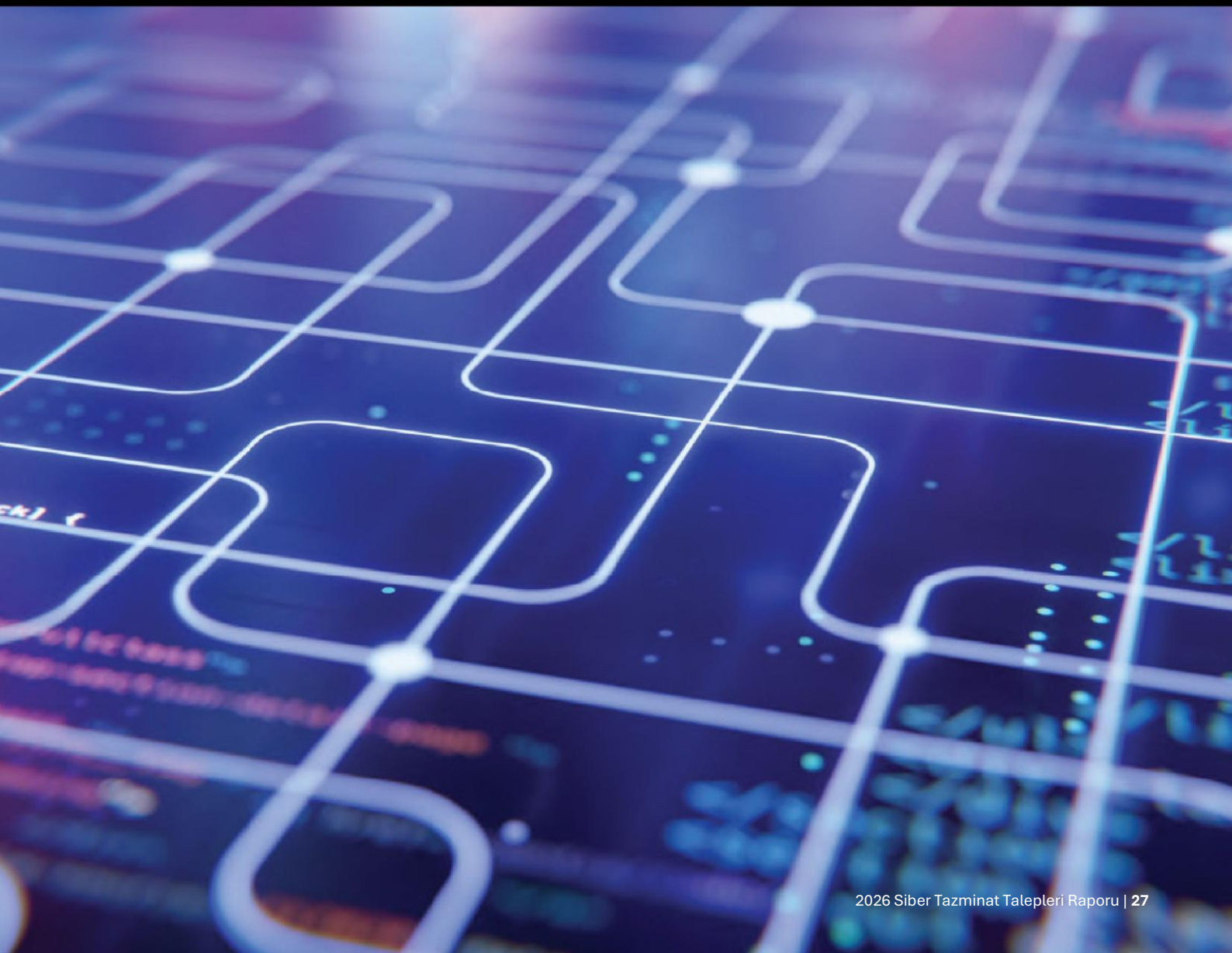
1,2 milyon $

Sonuç: Toplam kayıp 1,2 milyon $ oldu.

On Birinci Bölüm

Chubb: Şirketlerin siber riskleri azaltmalarına yardımcı olacak içgörüler sunuyor

Risk azaltma araçlarına ek olarak, bilgi de gelişen siber tehditlere karşı en güçlü savunmalardan biridir. Chubb, sigortalılara, siber vaka önleme ve azaltma desteği için çeşitli içgörüler sunar.



Chubb Cyber Index

2015 yılında hizmete sunulan Chubb Cyber Index, Chubb'ın küresel özel hasar verilerine ve güncel siber tehditler, eğilimler ile maliyetlere ilişkin içgörülere gerçek zamanlı erişim sağlar.

Aranabilir platform, kullanıcıların parametreler belirlemesine ve aşağıdaki kriterlere göre tarihsel eğilimleri görüntülemesine olanak tanır:

Vaka Aktivitesi: Organizasyonları etkileyen siber tehdit trendleri büyüklüğe, endüstriye ve coğrafi bölgeye göre ayrılır.

Hasar Tutarları: Chubb siber tazminat taleplerini, hasar tutarlarına, organizasyon büyüklüğüne ve endüstriye göre ayrılır.

Siber Risk Hesaplayıcısı: Siber tehditlere açıklık spektrumu ve potansiyel siber kayıp maliyetlerine dair içgörüler sağlayan bir araçtır.

Emsal Satın Alma İçgörüleri: Şirketlerin kendi siber koruma düzeylerini benzer kuruluşlarla karşılaştırarak değerlendirmelerine olanak tanıyan bir araçtır.

Kimlik Avı/Sosyal Mühendislik
Güvenlik Açığı
Şirket Dışı Uzak Hizmetler
Diğer Taktik

2022 yılına kıyasla, ciddi güvenlik açığı istismarlarından kaynaklanan taleplerin oranı yaklaşık %22'den %9'a gerilemiştir; bu düşüş, Chubb'ın Siber Tehdit İstihbaratı ekibinin en kritik istismar edilebilir güvenlik açıklarını önceliklendirdiği ve yalnızca bu güvenlik açıklarından potansiyel olarak etkilenebilecek sigortalılara hedefli uyarılar sunduğu Güvenlik Açığı Yönetimi Bilgilendirme Programı'nın devreye alınmasıyla örtüşmektedir. Bu hizmet, tüm Chubb Cyber sigortalılarına ücretsiz olarak sunulmaktadır.

Chubb Tehdit İstihbaratı

Siber Tazminat Talepleri Raporumuza ek olarak, siber profesyonellerine siber tehditlerdeki son gelişmeler hakkında kısa ve harekete geçilebilir içgörüler sağlamak için üç aylık Tehdit İstihbaratı Raporu ve Chubb tazminat talebi deneyimi de sunuyoruz.

Son bir rapor, 2025 yılında fidye yazılımı olayına yol açan en yaygın ilk erişim taktiğinin oltalama (phishing) olduğunu göstermiştir. Harici uzaktan hizmet istismarı (örneğin VPN suistimali, açık portlar) ikinci sırada yer alırken, ciddi güvenlik açığı istismarları üçüncü sırada gelmiştir.

Chubb, Güvenlik Açığı Yönetimi Bilgilendirme Programı (Vulnerability Management Outreach Programme) aracılığıyla, portföyümüzü sürekli olarak tarar ve yenileme sırasında veya poliçe döneminde aracıları ve poliçe sahiplerini, kapatılması gereken ciddi, suistimal edilebilir sorunlar hakkında bilgilendirir. Hizmet, tüm Chubb Siber poliçe sahiplerine ücretsiz olarak sunuluyor.

Güvenlik Açığı Yönetimi Bilgilendirme Programımıza ek olarak Chubb, sigortalıların kimlik avı saldırılarına karşı risklerini azaltmalarına yardımcı olmak üzere özellikle oltalama odaklı hizmetler de sunmaktadır; bunlar arasında:

Eğitim

Çalışanlar için güvenlik farkındalığı ve en son tehditleri temel alan kimlik avı önleme kursları ve oyunları.

Test

Çalışanların karar verme davranışlarını test eden, derin sahte montaj teknolojisi simülasyonlarını da içeren kimlik avı e-postası simülasyonları.

Teknoloji

Bir insanın fark etmesinin muhtemel olmadığı kimlik avı amacını, dili ve davranışsal anormallikleri tespit etmeye yardımcı olan yapay zekâ destekli bir e-posta güvenlik aracı.

On İkinci Bölüm

Sonuç

Hızlanma Çağında Dayanıklılık

2025 yılındaki siber risk, hızlanma ile tanımlanmıştır. Otonom yapay zeka saldırıları, genişletilmiş gizlilik düzenlemeleri ve toplu tahkim taktikleri, zaman aralıklarını daraltan ve potansiyel siber vaka sonuçlarını şiddetlendiren etkenler arasında yer almaktadır.

Gelişmiş tespit kabiliyetlerine yatırım yapmak, yapay zekâ ve veri uygulamaları üzerindeki yönetimi güçlendirmek ve üçüncü taraf ekosistemleri stres testine tabi tutmak, kuruluşların kırılganlıklarını önemli ölçüde azaltabilecek birçok yöntemden bazılarıdır.

Onlarca yıldır yaptığımız gibi Chubb yardıma hazır. Küresel deneyimimiz, detaylı tazminat talebi verilerimiz ve entegre risk azaltma ve müdahale becerilerimiz, müşterilerimizin günümüzün karmaşık siber olaylarını öngörmelerine, bunlara dayanmalarına ve saldırı sonrası toparlanmalarına destek olduğu gibi geleceğe de hazırlanmalarına yardımcı olur. Dünyanın her yerinden müşterilerimizle çalışmayı, siber risklere karşı finansal ve operasyonel dayanıklılık inşa etmeyi sabırsızlıkla bekliyoruz.

Daha fazla bilgi almak için
Chubb Siber Sigorta
sayfasını ziyaret edin

CHUBB®

Kapsamlı siber koruma ve dayanıklılık için Chubb'a güvenin.

Chubb European Group SE Merkezi İngiltere Türkiye İstanbul Şubesi, Büyükdere caddesi no 100-102, Maya Akar Center B Blok Kat:5, Esentepe 34394, İstanbul, Türkiye 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 tabidir. Chubb, çeşitli müşteri gruplarına kurumsal ve bireysel mal ve kaza sigortası, ferdi kaza ve tamamlayıcı sağlık sigortası, reasürans ve hayat sigortası ürünleri sunan bir küresel liderdir. Ana şirket Chubb Limited, New York Borsasına kotedir (NYSE: CB) ve S&P 500 endeksinde yer almaktadır.