Katastrofik Siber Riskler – Büyüyen Bir Endişe

CHUBB

Dünya dijitalleştikçe siber olayların sıklığı, şiddeti ve karmaşıklığı, teknolojiye bağımlılıkla beraber artmaktadır. Güvenlik açıkları ve tehlikeler, teknolojik bağlantı sayısındaki artış nedeniyle çoğalmakta ve giderek artan, büyüyen, tespit ve kontrolü zor sistemik riskler oluşturmaktadır. Bu sistemik risk boyutları ciddi ve geniş çaplı sorunlara yol açabilecek sonuçlarla birlikte düşünüldüğünde ortaya bir Katastrofik Siber Felaket olasılığı çıkmaktadır.

Tıpkı pandemilerde olduğu gibi siber olaylar da zaman veya coğrafya ile sınırlı olmayan kayıplara yol açabilir. Bu artık teorik değil. Siber suçlular, özellikle yakın zamanda meydana gelen Colonial Pipeline'ın ABD'nin doğu kıyısına yakıt tedarik eden boru hatlarının devreden çıkarılmasıyla sonuçlanan son saldırıda dünyanın dört bir yanındaki işletmeler için tedarik zincirlerini bozma ve kritik altyapıyı sakatlama yeteneklerini kanıtladılar. Dünyanın dört bir yanındaki işletmelerin tedarik zincirlerini kesintiye uğratan ve teknik altyapıyı bozan bir saldırıdır. Bu riskler göz önüne alındığında artık sigorta sektörünün bilanço kapasitesini sınayabilecek Katastrofik niteliğindeki bir saldırıyı hayal etmek pek de zor değil.

Daha önce aniden gerçekleşen yıkıcı olayların aksine siber risklerin devamlı yukarı tırmanışına şahit oluyoruz. Bunun önceden bilinmesi bir Katastrofik meydana gelmeden önce siber koruma ve ekonomik önlemler oluşturma fırsatı tanımaktadır.

Siber Sigorta Gerekliliğini Kanıtladı

Son yıllarda, önemli siber olaylar sonrasında dünya genelinde çok sayıda kurumun sigorta şirketlerinin koruması altında kayıplarının karşılanmasıyla birlikte siber sigorta hizmeti tam olarak yerine getirilmiş oldu.

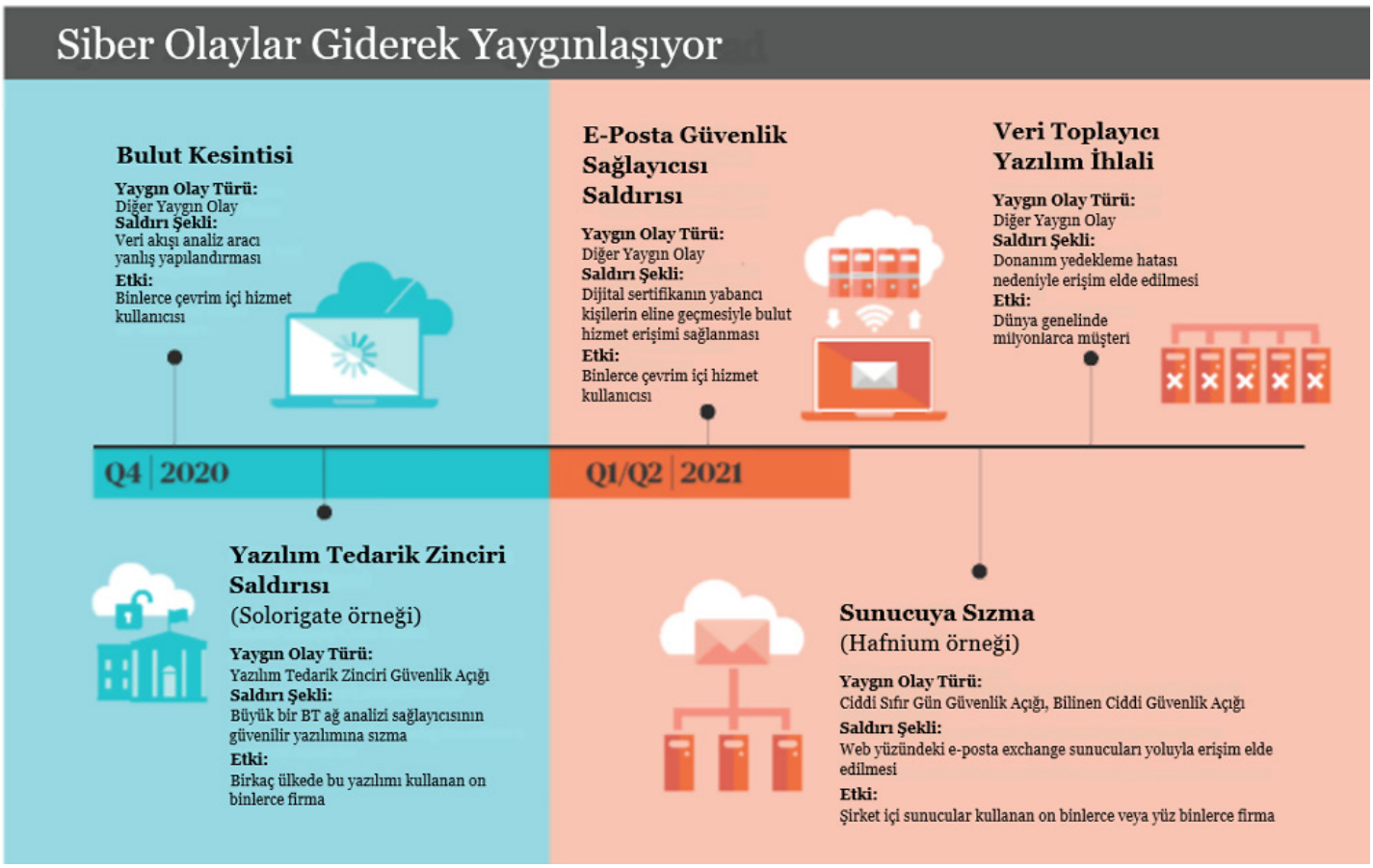
Günümüzde siber saldırı olayına müdahale masrafları, birinci taraf siber riski, üçüncü taraf siber sorumluluğu ve mesleki sorumluluk/hatalar ve ihmalleri kapsayan temel teminatlar, ölçeği ve sektörü fark etmeksizin tüm kurumlara yönelik önemli risk devir ve risk yönetim çözümleri sağlamaktadır. Aynı zamanda, sigorta şirketleri tarafından sunulan siber risk yönetim hizmetleri şirketlerin riskleri azaltmalarına ve ön uçtaki teknoloji önlemlerini iyileştirmelerine önemli bir katkıda bulunmuş ve diğer yandan olay müdahale ekipleri de şirketlerin bir siber olay sonrası daha kısa sürede çevrim içi olmalarını sağlama konusunda etkili olmuştur.

Siber sigorta yaptıran kurum sayısının giderek artması (Mayıs 2021'de yayınlanan Hükümet Sorumluluk Ofisi raporuna göre şu anda ABD'de ikamet eden ve ABD dışındaki eksedan grup sigorta şirketleri açısından yaklaşık 4 milyon poliçe olduğu ve ABD'deki işletmelerin neredeyse yüzde 50'sinin teminat altına alındığı tahmin edilmektedir) daha fazla şirketin

korunduğu anlamına gelmekte ancak aynı zamanda, sigorta sektörü için siber risk kapsamının genişlediğini de göstermektedir.

Bununla birlikte, şirketler son birkaç yıl içinde siber dayanıklılıklarını da geliştirmiştir. 2020'de dünya genelindeki bir ankete katılan BT ve güvenlik uzmanlarının yüzde 53'ü kurumlarının yüksek bir siber dayanıklılık düzeyine ulaştığını belirtmiştir (bu oran 2015'te ise yüzde 35 olarak belirlenmişti).

Siber sigortanın, kurumların siber riskleri yönetmeleri konusunda giderek artan önemde bir rol oynadığı açık olmakla birlikte sigortacıların uzun vadede olası toplam zararı karşılayıp karşılayamayacağı o kadar net değildir.



Artan Riskler ve Etki

Kurumların siber risk ve bunun sonuçları konusunda daha bilgili olmasına karşın siber olaylar ve tehditler artmaya ve şekil değiştirmeye devam etmektedir.

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. 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. 2020'de meydana gelen başarılı güvenlik ihlallerinin %85'i sosyal mühendislik uygulamaları gibi bir insan unsuru içermekteydi.

Fidye yazılımı gibi taktikler daha yaygın ve maliyetli olmakla beraber işle ilgili e-posta tehlikeleri ve veri ihlalleri, özellikle COVID-19 pandemisinde ve bunun sonucunda gerçekleşen kapsamlı uzaktan çalışma düzenlemeleri sırasında siber olay görülme sıklığını hiç olmadığı kadar yüksek seviyelere taşımaya devam etmektedir.

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 100.000'i aşkın kuruluş bu olaylardan etkilenmiştir.

Örneğin, Solorigate olarak bilinen bir olayda, güvenilir bir ağ analizi yazılımının güncellemesine yerleştirilen kötü amaçlı bir kodun neredeyse sekiz ay boyunca fark edilmemesi sonucunda meydana gelen büyük bir tedarik zinciri saldırısından yaklaşık 20.000 şirket ve devlet kurumunun etkilendiği ortaya çıkmıştır.

Başka bir olayda ise ulus devlet aktörleri ve suç örgütlerinden oluştuğu iddia edilen Hafnium adındaki bir grup neredeyse yüz binlerce firmanın tesislerindeki sunuculara erişmek için yaygın bir yazılımdaki o zaman bilinmeyen ("sıfır gün") güvenlik açığını kullanmıştır.

Sansasyonel Olaylar Gerilimi Artırıyor

Solorigate ve Hafnium olayları her ne kadar yaygın ve maliyetli olsa da bunların etkisi çok daha kötü olabilirdi. Bu olayların her birinin ortaya çıkmasındaki birincil etken casusluk gibi görünmektedir fakat amaç, kritik verileri veya diğer bilgileri çalmak veya yok etmek olsaydı ekonomik sonuçlar muhtemelen kat be kat fazla olurdu. FireEye adlı siber güvenlik firmasının CEO'su Kevin Mandia'nin Senato İstihbarat Komitesi'ne verdiği ifadeye göre Solorigate saldırısının arkasındaki kötü niyetli kişiler yıkıcı olmak isteselerdi bunun için gerekli erişim ve yeteneğe sahiplerdi.

Bir örnek daha vermek gerekirse 2017'de NotPetya saldırısı neredeyse sadece Ukrayna'da kullanılan M.E.Doc adlı bir vergi yazılım aracındaki güvenlik açığını suistimal etmiş ancak daha sonra bu kötü amaçlı kod rastgele yayılarak nihayetinde Avrupa, ABD ve diğer yerlerde bulunan birçok büyük şirketi etkilemiş ve tahmini 10 milyar ABD doları tutarında bir zarara yol açmıştır. NotPetya saldırısından mağdur olan bazı şirketler 100 milyon ABD dolarını aşan zararlara maruz kalmıştır. Solorigate veya Hafnium saldırılarında bu tür yıkıcı bir kötü amaçlı kod kullanılmış olsaydı toplam ekonomik zarar NotPetya olayından kat be kat büyük olabilirdi.

Aynı yıl gerçekleşen WannaCry isimli bir fidye yazılımı saldırısı ise dünya genelinde 200.000'den fazla bilgisayarı etkilemiştir. Saldırıda neyse ki halihazırda yaması olan, bilinen bir güvenlik açığı kullanılmıştı; dolayısıyla birçok kullanıcı buna karşı hazırlıklıydı. Ancak, yukarıda bahsettiğimiz Hafnium örneğinde olduğu gibi, saldırı bir sıfır gün güvenlik açığını suistimal etmiş olsaydı bunun çok daha geniş çaplı ve ciddi etkileri olabilirdi.

Şimdiye kadar yaygın olaylara (örn. Solorigate ve Hafnium) ve yıkıcı olaylara (örn. NotPetya ve WannaCry) şahit olmuş olsak da bu olayların yol açtığı kayıplar hep yönetilebilir oldu. Peki böylesine büyük bir kayıp potansiyeli varken hem yaygın hem de yıkıcı olan tam anlamıyla Katastrofik niteliğindeki bir siber olayla ne zaman karşılaşacağız?

Olası Katastrofik Niteliğindeki Siber Olaylar

Kurumlar ve tüketicilerin giderek artan orandaki teknoloji bağımlılığının yanı sıra teknolojiler ile ortakların birbirine bağlı olması, siber olayların ciddiyetinin katlanarak büyüyebileceği bir ortama zemin hazırladı. Aşağıdaki olay türlerinin, özellikle kombinasyon halinde karşımıza çıktığında Katastrofik niteliğinde olaylara dönüşme potansiyeline sahip oldukları tespit edilmiştir.

Yaygın Ağır Bilinen Güvenlik Açıkları:
Günde ortalama yaklaşık 50 yeni yazılım güvenlik açığı yayınlanmaktadır. Yamalar uygulanmazsa bu güvenlik açıkları suistimal edilebilir. Suistimal edilmelerinin kolay olması, sınırlı erişim öncelikleriyle uzaktan dağıtılabilmesi ve önemli olumsuz etkilere sebep olabilmeleri nedeniyle bunların yaklaşık %15'i ciddidir. Ciddi güvenlik açıkları geniş çapta bilindiği ve genel internet taraması teknikleriyle potansiyel mağdurların ağlarında tanımlanabildiği için bu ciddi yazılım güvenlik açıkları üzerinde durmayan şirketlerin mağdur olma riski çok yüksektir.

Yaygın ve Ağır Sıfır Gün Güvenlik Açıkları:
Sıfır gün yazılım güvenlik açıkları siber suçlular arasında bilinmekte ancak henüz başkaları tarafından bilinmemektedir. Bunlar bilhassa endişe vericidir çünkü bazıları kolayca suistimal edilebilir durumdadır, ciddi olabilir ve genellikle koruyucu önlemleri yoktur. Diğer bir deyişle, iyi çalışan siber risk yönetim programları olan şirketler bile sıfır gün saldırılarına maruz kalabilir.

Yazılım Tedarik Zinciri Güvenlik Açıkları:
Yazılım tedarik zinciri saldırıları temelde kötü niyetli kişilerin güvenilir, sertifikalı yazılımlar aracılığıyla sistemlere girmesine izin veren bir Truva atından doğar. Solorigate operasyonunda saldırganlar, teknoloji sektöründe yaygın şekilde kullanılan yazılım geliştirme uygulamalarını suistimal ederek karmaşıklık seviyesi yüksek bir saldırı ortaya koymuştur. Çoğu devlet aktörleri tarafından yön verilen veya sponsor olunan saldırılar izlenimi uyandıran bu saldırıların devam etmesi ve hızlanabilmesi beklenmektedir. Özellikle Batı ile düşmanları arasındaki jeopolitik sürtüşme bu olayların ileriye dönük tehdidini şiddetlendirmeye devam edecektir.

Altyapı Kesintileri:
Altyapının dahil olduğu saldırılar ve diğer siber olaylar geniş çaplı sonuçlar doğurabilir. Örneğin, ABD'nin doğu kıyısına hizmet veren benzin tedarik şirketi Colonial Pipeline'a Mayıs 2021'de yapılan saldırıda yabancı siber suçlular bir fidye yazılımı saldırısı yoluyla altyapı kesintisinden yararlanarak etkinin şiddetini artırmıştır. Sonuç olarak, boru hattı birkaç gün kapalı kalmış ve Amerika'nın yakıt tedarikini yüzde 45 oranında etkileyerek birçok eyalette milyonlarca vatandaş ve işletme için yakıt kıtlığına neden olmuştur. Altyapı kesintisi riski, sadece bir siber saldırıdan değil aynı zamanda sistem arızaları, insan hataları, programlama hataları veya diğer kötü amaçlı olmayan siber olaylardan da kaynaklanabilmesi nedeniyle farklı bir yapıdadır.

Diğer Yaygın Olaylar:
Belirli türdeki siber saldırılar çok sayıda mağduru hedef alıp eş zamanlı veya otomatik olarak gerçekleştirilebilir. İnternet ve bazı telekomünikasyon hizmetleri günümüzde kritik toplumsal altyapılar haline gelmiş ve bu da olası bir arıza riskinin kapsamını muazzam bir boyuta taşımıştır. Bazı durumlarda bir telekomünikasyon şirketi büyük veya orta ölçekli bir şehir için tek sağlayıcı olabilmektedir. Başka durumlarda ise bazı büyük bulut bilişim firmaları o kadar yaygın kullanılmaktadır ki büyük bir kesinti aynı anda binlerce veya milyonlarca farklı şirketin ticari faaliyetlerini etkileyebilecek düzeydedir. Büyük bir yayılım kapasitesi olan bu tür bir saldırı Katastrofik niteliğinde bir siber olaya neden olabilir.

Fidye Yazılımı Olayları:
Yapısı gereği tam olarak Katastrofik niteliğinde olmasalar da hedeflenen kuruluşların veya kişilerin elektronik dosyalarını veya bilgilerini bir ücret ödenene kadar rehin tutan fidye yazılımı saldırıları artık otomatik bir etkinlikle gerçekleştirilmektedir. Binlerce dolardan başlayan tipik talepler şu anda on milyonlarca dolara fırlamış durumdadır ve suçlular tüm ölçeklerdeki kuruluşları hedeflemektedir.

Siber Dayanıklılığı Güçlendirme

Faaliyetlerin ve BT ortamlarının yapısı, ortak altyapı arızaları veya güvenlik açıklarını kullanan kötü niyetli kişiler sebebiyle gerçekleşen siber risklerin artmasıyla birlikte kuruluşların olası bir siber Katastrofike yönelik hazırlıklarını artırmaları her zamankinden daha kritik hale gelmiştir.

Her kuruluşun, bu yazıda ana hatlarıyla belirtilen Katastrofik niteliğindeki olası siber olayları inceleyerek, karşılaşabileceği belirli riskleri anlaması ve ardından siber savunmasını ve dayanıklılığını geliştirmek için gerekli kaynakları belirlemesi başlangıç için atılabilecek iyi bir adımdır. Ortak BT sağlayıcıları kurumlar için önemli bir sistemik risk teşkil etmektedir; bu nedenle, bu sağlayıcılar için kapsamlı bir durum tespiti yapılmalı ve bu kapsamda, yedekleme ve dayanıklılık oluşturulup riskin nasıl devredileceğini görmek için sözleşmelerdeki tazminata ilişkin maddeler de gözden geçirilmelidir.

Kurumlar aynı zamanda sigorta brokerleri veya acenteleri ve siber sigorta şirketleri tarafından sunulan uzmanlıktan da tam olarak faydalanmalıdır. BT, risk yönetimi ve iş sürekliliği ekipleri siber korumaları ve olay müdahale önlemleri konusunda kendilerine güvenseler de hiçbir kuruluş tüm olası siber olaylara, özellikle de Katastrofik niteliğinde olanlara karşı tamamen korunamaz.

Birçok sigorta şirketi, kuruluşların siber savunma durumunu iyileştirmelerine yardımcı olmak için müdahaleye hazırlık değerlendirmeleri, güvenlik performansı kıyaslamaları, ağ güvenlik açığı testleri ve yaygın saldırı simülasyonları gibi çeşitli olay öncesi hizmetleri sunmaktadır. Kuruluşlar ayrıca bir siber olay meydana geldiğinde müdahale etmeye de hazırlıklı olmalıdır. Bir sigortacının uzmanlardan oluşan olay müdahale ekibi bu tür olaylarda zararı kontrol altına almaya ve kuruluşun mümkün olan en kısa sürede yeniden tam faaliyet göstermesine yardımcı olabilir. Bu hizmetler, büyük bir siber olayı atlatma ile güvenle işlere devam etme arasında fark yaratabilir.

Gelişen Çözümler

Küresel bir perspektiften bakıldığında Katastrofik niteliğindeki siber olaylar ticareti durma noktasına getirme ve kritik altyapıları aksatma potansiyeline sahiptir. Tıpkı koronavirüs pandemisinde olduğu gibi bu durum, devletin ve özel sektörün birlikte çalışmasını gerektirmektedir. Bu anlamda yapılacak bir iş birliği kapsamında veri tutarlılığını geliştirmeye yönelik olarak siber olayların açıklanması ve raporlanması ve siber suçluları caydırmaya ve cezalandırmaya yönelik yasal çerçeveler belirlenmesi gibi önemli konular yer almaktadır.

Siber olayların sıklığı ve şiddetinin artması, sigortacıların, fiyat politikaları ile şart ve koşullarını yeniden değerlendirmelerine neden oluyor. Katastrofik niteliğindeki risklerin potansiyel ölçeğini hesaba katarak siber sigorta için istikrarlı bir pazar sağlanması örneğin, bireysel sigortacıların ürün tekliflerine ilişkin ve hükümetle yapılacak iş birliklerine dair yeni çözümler sunulmasını gerektirecektir. Sigorta sektörünün önündeki zorluk ise gerek müşteriler gerekse sigortacılar açısından teminat netliği sunan, anlamlı bir koruma sağlayan ve hem yıpratıcı hem de Katastrofik niteliğindeki siber olayların yönetilmesine yardımcı olan poliçelerin nasıl hazırlanacağıdır.

Sigortacılar, geçmişte, sel ve deprem gibi Katastrofiklere karşı gayrimenkulleri, bunlara ilişkin risk düzeylerini hem şeffaf bir şekilde fiyatlandırmak hem de izlemek için ayrı bir teminat kapsamında teminat altına almışlardır. Bu süreç, genel pazar istikrarının ve teminat mevcudiyetinin korunmasına yardımcı olmuştur. Örneğin, son 50 yılda meydana gelen deprem, sel ve kasırga gibi birçok büyük olay mal ve kaza sigortası sektöründe kazanç anlamında önemli olayları teşkil etmekle beraber bunlar nadiren sigorta şirketlerinin iflasına yol açmıştır. Sonuç olarak sigorta sektörü, Katastrofiklerden sonra dahi poliçe sahipleri için dayanıklı ve istikrarlı kalabilmiştir.

Mal sigortası gibi siber sigorta da Katastrofik niteliğindeki olaylara karşı risk altındadır ve bu nedenle siber sigorta sektörünün mal sigortası sektörü ile aynı şekilde yanıt vermesi gerekebilir. Sektörün, temel teminatlardan ayrı olarak Katastrofik niteliğindeki olaylara yönelik teminat sunma konusunda proaktif olması gerekir. Katastrofik niteliğindeki olaylara yönelik teminatın hariç tutulmaması ve bununla birlikte, ayrıca sunulacak teminatın şeffaf bir şekilde fiyatlandırılması ve uygun sigortalama, teminat limitleri ve müşteri konservasyonuna tabi olması bağlamında daha net bir şekilde belirtilmesi gerekir. Bu yaklaşım, siber sigorta sektörünün poliçe sahiplerine yenilikçi çözümler sunmaya devam etmesine imkan vermekle kalmayıp pazarın uzun vadeli sürdürülebilirliğini de sağlayacaktır.

Yazar Hakkında

Michael Kessler, Chubb Group Başkan Yardımcısı ve Chubb Küresel Siber Risk Uygulaması Bölüm Başkanıdır. Bu görevleri kapsamında Bay Kessler; strateji, ürün ve iş geliştirme, sigortalama ve hizmet faaliyetleri ile genel kâr-zarar performansı da dahil olmak üzere işletmeyi tüm yönleriyle denetler. Bay Kessler sigorta ve aktüerya danışmanlığı alanında yaklaşık 30 yıllık bir deneyime sahiptir ve daha önce Chubb'ın Baş Reasürans Sorumlusu (2016-2021) ve uluslararası sigorta kolunun Baş Aktüeri (2008-2016) olarak görev yapmıştır. Bay Kessler, Cornell Üniversitesi (Cornell University) matematik lisans bölümü mezunudur. Amerikan Aktüerler Akademisi (American Academy of Actuaries) ve Kaza Aktüeryası Birliği (Casualty Actuarial Society) üyesidir.

son notlar

1. Siber Sigorta: Sigortacılar ve Poliçe Sahipleri Sürekli Değişen bir Pazarda Zorluklarla Karşı Karşıya (2021). www.gao.gov/products/gao-21-477
2. Siber Dayanıklılık Kurum Raporu (2020). www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/
3. National Institute of Standards and Technology Ulusal Güvenlik Açıkları Veri Tabanı. https://nvd.nist.gov/vuln/search
4. AV-TEST Institute (2021). www.av-test.org/en/statistics/malware/
5. Verizon'un 2021 Veri İhlali Araştırmaları Raporu (2021). https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf
6. ABD Senatosu İstihbarat Seçilmiş Komitesi (2021). www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary
7. NIST Security Vulnerability Trends in 2020: An Analysis (2021). www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

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 ve en hızlı şekilde yanıt verir ve gerekli ödemeleri yaparız. Şirketimiz aynı zamanda kapsamlı ürün ve hizmet teklifleri, geniş dağıtım kapasitesi, olağanüstü mali gücü ve küresel çapta yerel operasyonları ile tanımlanmaktadır. Chubb'ın ana şirketi olan Chubb Limited, New York Borsası'na kotedir (NYSE: CB) ve S&P 500 endeksinde yer almaktadır. Chubb'ın Zürih, New York, Londra, Paris ve diğer şehirlerde bulunan idari ofislerinde dünya genelinde yaklaşık 31.000 kişi istihdam edilmektedir. Daha fazla bilgi için: www.chubb.com.

Chubb'ın siber risk yönetimine ilişkin deneyimi ve uzmanlığı hakkında daha fazla bilgi almak için Chubb Türkiye Siber sigortalar Underwriter'ı Meltem Yılmaz ile meltem.yilmaz@chubb.com adresinden irtibata geçebilirsiniz.

Chubb. Insured.℠

TR8127-MD 02/22