Digitale Wertschöpfung in Gefahr: Blackout durch das Cyber-Risiko DDoS?

Die digitale Autobahn wird zum Flaschenhals: Wenn „Denial of Service"-Attacken den Datenverkehr zum Stillstand bringen, droht der Kollaps für die vernetzten Use Cases von heute. Unternehmen müssen das massiv zunehmende Risiko ernst nehmen und umgehend handeln.

Die Digitalisierung ist eine atemberaubende Erfolgsgeschichte. Mit den leistungsfähigen innovativen Technologien und dem Siegeszug der neuen Geschäftsmodelle steigt aber zugleich auch die Verwundbarkeit der Unternehmen. Durch Ansätze wie Cloud, IoT, KI und Echtzeit-Anwendungen wachsen die Datenströme, die Komplexität nimmt zu, und ebenso die Zahl der möglichen Angriffsflächen für weitreichende Cyber-Attacken. Vor allem aber auch der potenzielle Schaden, den diese anrichten können. Schließlich basieren heute viel mehr kritische Bausteine in den Wertschöpfungsketten auf digitalen Ansätzen als noch vor wenigen Jahren. 2021 stellen laut AXA Future Risks Report Cyber-Risiken das zweitwichtigste Top-Risiko weltweit dar. „Erfolgreiche Digitalisierung braucht Cyber-Sicherheit", resümiert daher das Bundesamt für Sicherheit in der Informationstechnik (BSI) und warnt in seinem aktuellen Sicherheits-Bericht vor den digitalen Gefahren. Neben den in der Öffentlichkeit bereits viel diskutierten Ransomware-Vorfällen sind es insbesondere Distributed-Denial-of-Service-Angriffe (DDoS), die große Schäden verursachen.

Dabei werden IT-Ressourcen wie etwa Server durch massenhafte missbräuchliche Anfragen in die Knie gezwungen, bis sie zusammenbrechen und ein Datenaustausch nicht mehr möglich ist. Einer der bekanntesten Fälle dieser Art in der letzten Zeit war der DDoS-Angriff auf die Börse Neuseeland im August 2020, der zu einem mehrtägigen Handelsausfall führte. Wie stark sich die Bedrohungslage zuspitzt, hat das BSI erst vor kurzem erneut unterstrichen: Für das Retail-Aufkommen rund um den Black Friday 2021 warnte es spezifisch vor einer akut erhöhten DDoS-Gefahr. Tatsächlich nahm die DDoS-Aktivität am Black Friday und am Cyber Monday gegenüber dem Vorjahr dann auch um 200 Prozent zu.

Das Bewusstsein für die DDoS-Problematik hinkt allerdings derzeit dem rapiden Wachstum dieser Spielart der Cyber-Kriminalität immer noch hinterher. In diesem Point of View wollen wir daher das Risiko durch DDoS-Attacken näher beleuchten und mögliche Abwehrmethoden aufzeigen. Denn erst wenn Art und Schwere der Bedrohung erkannt sind, können auch zielführende Maßnahmen zum Aufbau nachhaltiger Cyber-Resilienz ergriffen werden. Das Cyber-Risiko für die deutsche Wirtschaft ist dabei keine abstrakte Größe. Laut einer Studie des Branchenverbands Bitkom entstand ihr 2020/21 durch Cyber-Vorfälle die erhebliche Schadenssumme von 220 Milliarden Euro. Gegenüber 2018/19 hat sich dieser Betrag mehr als verdoppelt. Es liegt auf der Hand, dass Unternehmen auf diesem Feld dringend verstärkt tätig werden müssen.

Die Bedrohungslage: DDoS-Attacken als eines der Top-Risiken

Das Arsenal der Cyber-Kriminellen ist mit einer breiten Palette von unterschiedlichen Angriffsmethoden gefüllt, die technologisch immer weiter verfeinert werden. DDoS-Angriffe haben sich in der Bitkom-Rangliste der schädlichsten Methoden inzwischen mit 27 Prozent den zweiten Platz gesichert, direkt nach Ransomware (31%). Während das DDoS-Segment heute

„DDoS-Angriffe weisen beunruhigende und rekordverdächtige Wachstumsraten auf. Sie stehen inzwischen schon auf dem zweiten Platz der Cyber-Risiken."

Marc Wilczek, Chief Operating Officer Link11

Ransomware fast schon eingeholt hat, lag es 2018/2019 noch auf Platz 6 der Bedrohungen. Die Security-Experten von Link11 untermauern das wachsende Risiko in ihrem aktuellen DDoS-Report durch weitere Zahlen. So nahm im ersten Halbjahr 2021 die Anzahl der DDoS-Angriffe um 33 Prozent zu. Auch bei detaillierteren Metriken bestätigt sich der Trend. Das maximale Angriffsvolumen stieg um 36 Prozent, die maximale Paketrate um 147 Prozent. Gegenüber dem ersten Quartal verdoppelten sich dabei die besonders gefährlichen Hochvolumen-Attacken. Die Zahl der Angriffe insgesamt stieg allein im zweiten Quartal um 19 Prozent.

Was bedeutet diese Zahlen in der Realität der betroffenen Organisationen und ihrer Stakeholder? Oft führen die Attacken zu schweren Disruptionen, die weite Teile des Betriebs lahmlegen – mit potenziell katastrophalen Folgen insbesondere in kritischen Branchen wie Gesundheit oder Infrastruktur. Der DDoS-Report von Link11 stellt einige besonders aufsehenerregende Angriffe aus dem ersten Halbjahr 2021 vor. So behinderten im Januar DDoS-Attacken auf deutsche Schulplattformen den Pandemie-bedingten Distanzunterricht. In Großbritannien, USA, Deutschland und anderen Staaten wurden Webseiten zur Corona-Impftermin-Buchung angegriffen. Im Mai wurde eine geschäftspolitische Änderung bei Cyber-Versicherungen des AXA-Konzerns in Frankreich zum Anlass für eine Welle von DDoS- und Ransomware-Angriffen auf asiatische Niederlassungen. In Irland kam es nach breit angelegten Attacken auf Internetprovider zu vielen mehrstündigen Ausfällen bei führenden Webhosting-Anbietern. Im Juni verursachten DDoS-Attacken auf die Rechenzentren eines Dienstleisters Großstörungen beim Online-Banking der deutschen Genossenschaftsbanken.

Die Motivation der Täter hinter den DDoS-Aktivitäten ist dabei unterschiedlich. Oft geht es um kriminelle Erpressung (Geldforderungen), wobei das Entdeckungsrisiko vergleichsweise gering ist – für Täter aus der organisierten Kriminalität ein reizvolles Szenario. Durch arbeitsteilige kriminelle Geschäftsmodelle steigern sie dabei noch die Effektivität und Effizienz ihrer Attacken. In anderen Fällen liegen politische Motive vor („Hacktivisten"). Teils spielen geopolitische und nachrichtendienstliche Zusammenhänge eine Rolle, wobei manchmal auch avancierte Technologien eingesetzt werden, die eigentlich nur staatlichen Akteuren zu Verfügung stehen. Oft muss aber schlicht Sabotage aus purer Zerstörungslust oder aus persönlicher Rache als Beweggrund angenommen werden.

Neue Dimensionen der Verletzlichkeit

Die Zunahme von Cyber-Attacken im Allgemeinen und von DDoS-Angriffen im Besonderen ist zunächst durch die gewachsene Verletzlichkeit der Unternehmen zu erklären. Hier ist eine ganze Bandbreite von Treibern wirksam. Durch die hochgradig integrierten globalen Wertschöpfungsketten von heute können Unternehmen nicht nur direkt, sondern auch indirekt – beispielsweise als Kunden von betroffenen Dienstleistern – in Mitleidenschaft gezogen werden. Durch die fortgeschrittene Digitalisierung wirken sich IT-Probleme auch nicht mehr nur eingegrenzt auf bestimmte Bereiche aus, wie z.B. die Unternehmenswebseite, sondern potenziell auf den ganzen Betrieb. Dabei kann es zu gefährlichen Zahnradeffekten kommen, bei denen der Ausfall eines einzigen Bestandteils das ganze Räderwerk blockiert und zu einem Blackout führt. Oder auch zu einem Dominoeffekt, bei dem ein singulärer Vorfall eine potenziell katastrophale Kettenreaktion auslöst.

Unternehmen müssen sich heutzutage immer mehr mit Risiken auseinandersetzen, die nicht in ihrem eigenen Einflussbereich entstehen. Eine Ursache hierfür liegt in der Verlagerung von Diensten und Fähigkeiten in die Cloud und im Trend weg von On-Premise-Installationen. Hierzu hat die britische Versicherungsbörse Lloyds of London schon vor längerer Zeit errechnet, dass z.B. der Ausfall eines einzelnen großen Cloud Providers für drei bis sechs Tage alleine in den USA 15 Milliarden US-Dollar an volkswirtschaftlichem Schaden verursachen könnte. Die indirekte Verletzlichkeit erstreckt sich aber auch auf andere Felder, z.B. durch Ausfälle von Zahlungsdienstleistern. Traditionelle „Hardware"-Produzenten wie Unternehmen aus dem industriellen Bereich sind ebenfalls betroffen. Unter dem Paradigma von Industrie 4.0 verflechten sich Informationstechnologie (IT) und operationale Technologie (OT) zunehmend, und immer mehr dieser Unternehmen wandeln sich zu „as-a-service"-Anbietern. Die Verwundbarkeit steigt durch Ansätze wie Internet of Things (IoT) noch weiter, und sie dehnt sich durch die Vernetzung der Lieferketten und die Integration der Ökosystempartner auch über Unternehmensgrenzen hinaus. Viele Anwendungen sind heutzutage zudem auf Realtime-Daten angewiesen und dadurch verletzlicher.

> „Unternehmen haben zunehmend das Problem, dass Risiken auf sie einwirken, die durchaus substanziell werden können, aber diese Risiken außerhalb ihres eigenen Kontrollbereichs liegen."
>
> **Ralph Noll, Partner Cyber Risk Deloitte Deutschland**

Auch Privatpersonen spüren eine verstärkte Anfälligkeit gegenüber Cyber-Problemen, zumal seit der Corona-Krise und dem Boom im Remote Working. Besonders sensibel sind vernetzte E-Health-Anwendungen und -Geräte, da sie die Gesundheit der einzelnen Personen beeinflussen können. Hier bestehen zugleich hohe Datenschutzrisiken. Im Consumer-Bereich sind außerdem Produkte wie der Connected Car, Smart Devices (Fitness u.a.) und smarte Haushaltsgeräte potenziell betroffen. Zur Debatte steht hier nicht nur der sicherlich unangenehme Ausfall eines vernetzten Haushaltsgerätes, sondern ein manipulatives, womöglich vom Verbraucher unbemerktes Hijacking, das smarte Geräte zum Teil eines Botnetzes macht. Die Endgeräte werden dabei zu willfährigen, ferngesteuerten „Zombiearmeen", die für erpresserische DDoS-Attacken mobilisiert werden können. Die jüngste Meris-Attacke stützte sich z.B. auf ein Botnetz von 250.000 Geräten weltweit. Nicht zuletzt gerät durch die Digitalisierung von staatlichen Institutionen und bürger- bzw. wirtschaftsnahen Verwaltungsdienstleistungen (E-Government) auch die öffentliche Hand zusehends ins Visier der Täter.

Für Unternehmen ist es aufgrund ihrer hohen und weiter ansteigenden Verletzlichkeit von höchster Dringlichkeit, sich die damit verbundenen Risiken bewusst zu machen: nicht nur auf der unmittelbaren finanziellen und operativen Ebene, sondern auch im Hinblick auf Reputationsrisiken und Haftungsrisiken z.B. jenseits der Gewährleistung. Dazu kommen erhebliche regulatorische Risiken. Durch neue oder aktuell in der Entwicklung befindliche Regelwerke wie DSGVO, EU AI Act (künstliche Intelligenz) oder EU Digital Operational Resilience Act (DORA) sind bestimmte Verstöße mit hohen Strafen bewehrt.

Wachsende Komplexität und Professionalität der Angriffe

Der digitale Fortschritt steht natürlich auch bei den kriminellen Akteuren nicht still, was einen weiteren Faktor bei den enormen Zuwachsraten der DDoS-Attacken darstellt. Es zeigt sich eine verstärkte Effizienz und Effektivität der Angriffsmethoden durch Nutzung der Möglichkeiten der Digitalisierung auch auf der Seite der Angreifer. Eine konsequente Professionalisierung ist zu konstatieren – bis hin zu Cybercrime-as-a-Service. Dieses Konzept ermöglicht es auch Tätern ohne technologisches Know-how, DDoS-Fähigkeiten als Dienstleistung zu konsumieren und mit minimalem Aufwand Angriffe zu starten.

Die Komplexität der Angriffe steigt dabei in mehreren Hinsichten. Besonders stark wächst die Zahl der Multivektor-DDoS-Angriffe, bei denen verschiedene technische Schwachstellen auf Transport-, Applikations- und Protokollebene gleichzeitig attackiert werden (z.B. UDP, TCP). Sie machten im ersten Halbjahr 2021 65 Prozent der Attacken aus, während Angriffe mit nur einem Vektor gegenüber dem Vorjahreszeitraum von 48 auf 35 Prozent zurückgingen. Da jeder Vektor eigene Abwehrstrategien erfordert, steigt mit der Anzahl der Vektoren auch die Schwierigkeit der Verteidigung. Beobachtet wurden Angriffe mit bis zu zwölf Vektoren. Zwei Vektoren wurden in 45 Prozent der Fälle angegriffen, drei in 42 Prozent.

Eine weitere komplexe DDoS-Bedrohungsart entsteht durch sogenannte Reflection-Amplification-Attacken. Dabei handelt es sich um indirekte Multivektor-Attacken, bei denen bestimmte Servertypen und Dienste ausgenutzt werden, die unzureichend konfiguriert sind. Zunächst erhalten sie missbräuchliche Datenpakete in begrenztem Umfang zugespielt, diese leiten sie dann jedoch vielfach verstärkt an das eigentliche Ziel weiter. Am häufigsten wird dabei der DNS-Dienst missbraucht (42%), es folgt der Dienst DVR DHCPDiscovery mit 29 Prozent. Auch hier geht die kriminelle Innovation ständig weiter. Relativ neu sind z.B. Attacken über den Dienst Session Traversal Utilities for NAT (STUN), also auf STUN-Server, die die Kommunikation mit VoIP-Endgeräten (z.B. Telefonen) hinter Firewalls ermöglichen.

Die Effektivität von DDoS-Attacken lässt sich noch um ganze Größenordnungen steigern, wenn sie nicht über Standard-Bots, sondern über solche in der Cloud gefahren werden. 35 Prozent aller DDoS-Angriffe werden über diese Schiene ausgeführt. Dabei werden Server-Instanzen von Cloud-Providern über Schwachstellen kompromittiert und in Bots verwandelt, die aufgrund der vielen Cloud-Anbindungen nun ungleich wirksamer sind. Das mögliche Angriffsvolumen liegt dabei um bis zu tausendfach höher. Die betroffenen Kunden bemerken diese Zweckentfremdung häufig erst später. Cloud-Kapazitäten werden teilweise aber auch direkt von Kriminellen gemietet, wofür dann beispielsweise gestohlene Kreditkartendaten genutzt werden. Am häufigsten finden Cloud-DDoS-Attacken aus dem AWS-Dienst statt (Amazon, 27%), es folgen Google Cloud (15%) und Microsoft Azure (11%). Durch den anhalten Cloud-Boom ist damit zu rechnen, dass dieser Typ von Attacken weiter zunimmt.

„Zunehmend kombinieren die Cyber-Angreifer verschiedene Angriffsmethoden – Ransomware, DDoS und die Veröffentlichung gestohlener Unternehmensinformationen im Darknet – um den Druck zur Erpressung von Lösegeld zu erhöhen."

Ralph Noll, Partner Cyber Risk Deloitte Deutschland

Die Lücken in der bestehenden Abwehr

An sich sind DDoS-Angriffe keine neue Erfindung. Schon seit den Anfangstagen des Internets werden Überlastungsattacken gegen Server gefahren. Das darf aber nicht dazu verleiten, diesen Typ von Cyber-Kriminalität als überholt zu betrachten. Nicht zuletzt durch die beschriebene Komplexitätszunahme ist DDoS aktueller denn je. Zugleich reichen die üblichen Sicherheitsmaßnahmen angesichts der neuen Dimension der Bedrohung nicht mehr zur Abwehr aus. Viele Unternehmen verlassen sich auf den Standard-DDoS-Schutz, den ihre Telekomdienstleister anbieten. Dieser weist jedoch typischerweise eine Reihe von Schwächen auf. DDoS-Abwehr ist nicht die Kernkompetenz der Carrier. Der gebotene Schutz umfasst oft nicht alle nötigen Ebenen, ist schlecht konfigurierbar und kapazitätsmäßig nicht ausreichend für intensivere Angriffe. Im Ernstfall kommt es daher häufig zu einer Überforderung des Carriers, der sich dann womöglich für ein „Null-Routing" entscheidet, also ein komplettes Verwerfen des betreffenden Datenverkehrs über Tage – für den Kunden keine befriedigende Lösung. Ein Hintergrund ist auch, dass allein die Daten-Transferkosten im Angriffsfall die Abwehr für den Carrier schnell unwirtschaftlich machen. Umso mehr lohnt sich für Unternehmen vorab ein Blick in die Tarifbedingungen und SLAs. Außerdem besteht bei dieser Art des Schutzes das Risiko, im Fall eines DDoS-Angriffs auf den Provider selbst indirekt zum Opfer zu werden.

Als Alternative kommt eine Abwehr durch lokale Hardware zwar prinzipiell in Frage, ist aber mit extrem großem Aufwand verbunden. Gegenüber dem heute möglichen „Flächenbombardement" durch moderne DDoS-Attacken mit Volumina von bis zu über 1 Tbps sind typische 10Gb-Außenanbindungen von Unternehmen um ein Vielfaches überfordert und selbst Außenanbindungen mit 100 Gig hilflos überlastet. Dazu kommt die Notwendigkeit, rund um die Uhr einsatzbereite Spezialteams aufzustellen. Auch das häufig eingesetzte Generic Route Encapsulation Tunneling (GRE Tunneling) weist z.T. Schwächen bzw. Limitierungen auf, u.a. bei großen Datenmengen. Es bietet keine ausreichende Fehlerkorrektur, leidet unter instabiler Latenz und ist verlustanfällig. Auch niedrige Durchsatzraten und die Overhead-Zusatzlast durch das Tunneling sind Nachteile. Angesichts der rapide wachsenden Bedrohung und der Schwächen bestehender Schutzmechanismen ist es an der Zeit, ein neues Modell der DDoS-Bekämpfung einzuführen. Durch Cloud-basierte Dienste spezialisierter Anbieter wird es möglich, den ihrerseits Cloud-basierten Angreifern auf gleicher Augenhöhe zu begegnen und diese effizient abzuwehren.

Neue Ansätze für ein neues Bedrohungsniveau

Das DDoS-Risiko erreicht immer höhere quantitative und qualitative Stufen. Die Abwehr muss diese Entwicklung nicht nur nachvollziehen, sondern ihr perspektivisch sogar einen Schritt voraus sein. Dafür ist es nötig, sich von den überkommenen Security-Paradigmen zu lösen. Es sind moderne Cyber-Ansätze gefragt, wie z.B. Zero Trust, Automatisierung und Risiko-Orientierung. Bei Zero Trust wird eine fundamentale „Beweislastumkehr" vorgenommen: Grundsätzlich wird keinem Vorgang und Akteur mehr ohne Analyse vertraut, ungeachtet der Frage, ob er sich innerhalb oder außerhalb bestimmter Unternehmens-Perimeter befindet. Eine Automatisierung der Prozesse wird bei zukunftsweisenden DDoS-Sicherheitsansätzen wie dem von Link11 mit spezialisierten Algorithmen ermöglicht. Dahinter stecken ausgeklügelte technologische Methoden der künstlichen Intelligenz (KI) und des maschinellen Lernens (ML). Es findet keine klassische Pattern-Erkennung mehr statt, sondern eine automatisierte Realtime-Analyse von Anomalien im Traffic (Quellen, Pakete). Die Abwehr läuft auf dieser Grundlage wesentlich schneller und präziser. Die Cloud-basierten Leistungsreserven aus dedizierten Rechenzentren erlauben eine Behebung von Problemen in Echtzeit, die den bisherigen zeitaufwendigen „Patch/Fix"-Ansatz ablöst. Dies schafft die nötige Skalierbarkeit, um auch hochvolumige Angriffe abwehren zu können. Die Cloud-Basierung gewährleistet die nötige Redundanz, die beim Schutz gegen Serverausfälle durch Überlastung ein wichtiger Aspekt ist. Durch die internationale Verteilung des Traffics ist hierbei auch Geo-Redundanz sichergestellt. Daneben punktet das Cloud-basierte Deployment dabei auch mit einem vorteilhaften Kostenprofil und effektiver Kostenkontrolle. Die effiziente Ressourcenverwendung hat entscheidende qualitative Vorteile: Durch den intelligenten Ansatz wird eine prinzipielle Risiko-Orientierung mit entsprechender Ressourcen-Allokation möglich. Es werden individuelle, Risiko-spezifische Datenprofile für Unternehmen erstellt, und innerhalb des Unternehmens können sensible Risiken verstärkt geschützt werden.

Die Umsetzung in der Security-Praxis

Risiko-Orientierung als wesentlicher Erfolgsfaktor für die Erlangung von Resilienz gegenüber DDoS-Attacken erfordert eine umfassende Analyse besonders schützenswerter digitaler Assets von Unternehmen, die für die Kontinuität des Geschäftsbetriebs zentral sind. Die Evaluierung der Risiken sollte bei der praktischen Umsetzung in eine generelle Bestandsaufnahme des individuellen Cyber-Reifegrads eingebettet werden, um eine belastbare Basis für die Cyber-Strategie herauszuarbeiten. Dabei wird der gewählte Ansatz zugleich auf die allgemeine Unternehmensstrategie abgestimmt. Auch auf anderen Feldern sollten Cyber-relevante Maßnahmen umgesetzt werden, etwa im Bereich der physischen Sicherheit. Die Maßnahmen sind durch aussagekräftige Tests zu prüfen, War Gaming und andere Übungen verbessern die Cyber-Resilienz auch auf der personellen Ebene. Schließlich ist die technische und prozessuale Einbindung von neuen Security Providern in die bestehende Prozesslandschaft ein Thema, das bei der Aufstellung für eine zeitgemäße DDoS-Abwehr beachtet werden sollte. Für die Bewältigung bietet sich ein umfassendes, Cloud-basiertes DDoS-Angebot wie das von Link11 an, bei dessen Implementierung die Experten von Deloitte Unternehmen kompetent unterstützen. Deloitte hilft darüber hinaus auch dabei, die Maßnahmen in einen ganzheitlichen Ansatz zu integrieren, und bietet die dafür nötige Expertise in angrenzenden Cyber-Disziplinen. Deloitte ist im Bereich Cyber führend und verfügt über erprobte Angebote zu allen wichtigen Themen – Cyber-Strategie, Cloud, Data & Privacy, Identity, Emerging Technologies, Application Security und Detect & Response. Dabei kann auf die fundierte Expertise von über 250 spezialisierten Mitarbeitern, umfassende Branchenerfahrung in allen Sektoren und die internationale Kompetenz eines globalen Netzwerks zurückgegriffen werden. Somit ist sichergestellt, dass eine ganzheitliche Cyber-Aufstellung gelingt, wie sie für einen effektiven Umgang mit diesem massiv angestiegenen Risiko heutzutage unerlässlich ist.

„Im Zeitalter des Cyber Everywhere muss auch die Cyber Security in der Cloud stattfinden und digitale Assets durch eine massive Skalierbarkeit der Dienste schützen, die durch die zunehmend aggressiveren Angriffe nötig wird."

Ralph Noll, Partner Cyber Risk Deloitte Deutschland

Quellenverzeichnis

AXA: AXA Future Risks Report 2021
https://www.axa.com/en/press/publications/future-risks-report-2021

Bitkom: Angriffsziel deutsche Wirtschaft
https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

Bitkom: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie (Studienbericht 2018)
https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2021
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Bundesamt für Sicherheit in der Informationstechnik (BSI): DDoS-Entwicklungen vor Black Friday und Cyber Monday
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-269757-1032.pdf?__blob=publicationFile&v=3

CyberTalk: 250,000 strong DDoS botnet, "record shattering" attacks
https://www.cybertalk.org/2021/09/13/250000-strong-ddos-botnet-record-shattering-attacks/

Deloitte: Cyber Security Report 2021
https://www2.deloitte.com/de/de/pages/risk/articles/cyber-security-report.html

Deloitte: The Future of digital identity
https://www2.deloitte.com/global/en/pages/risk/articles/the-future-of-digital-identity.html

Deloitte: The trust enabler. Building cyber-security strategies for a trusted, digital future
https://www2.deloitte.com/us/en/insights/topics/digital-transformation/digital-trust-for-future.html

Deloitte Future of Cyber Risk 2035: Vier Zukunftsszenarien
https://www2.deloitte.com/de/de/pages/risk/articles/future-of-cyber-risk-2035.html

Deloitte: Zero Trust. Paradigmenwechsel in der Cybersecurity
https://www2.deloitte.com/de/de/pages/risk/articles/zero-trust.html

Link11: Distributed Denial of Service Report für das 1. Halbjahr 2021
https://www.link11.com/de/downloads/ddos-report-h1-2021

Link11: Record Number of Cyber Attacks over Black Friday
https://www.link11.com/en/blog/threat-landscape/record-number-of-cyber-attacks-over-black-friday-weekend/

Lloyd's: Failure of a top cloud service provider could cost US economy $15 billion
https://www.lloyds.com/about-lloyds/media-centre/press-releases/failure-of-a-top-cloud-service-provider-could-cost-us-economy-15-billion-dollars

Ihre Ansprechpartner

Ralph Noll
Partner | Risk Advisory
Tel: +49 211 8772 2285
rnoll@deloitte.de

Deloitte.

Stand 02/2022