LINK11

WHITEPAPER

DDoS, Datenschutz und die neuen Anforderungen für Schweizer Unternehmen

www.link11.com

In Kooperation mit:

bratschi

LINK11

Inhalt

Cyber-Risiko DDoS

Swiss Cyber-Security: DDoS, Datenschutz und die neuen Anforderungen für Schweizer Unternehmen

Rasant ansteigende Cybercrime-Fälle und neue Meldepflichten bei Datensicherheitsverletzungen gemäss revidiertem schweizerischem Datenschutzgesetz verstärken Handlungsbedarf bei Schweizer Unternehmen.

Über das Internet vernetzte IT-Systeme bilden die Basis für die Digitalisierung Schweizer Unternehmen. Doch auch Kriminelle nutzen die Vernetzung für sich, um gezielt Unternehmen anzugreifen und zu schädigen. Viele Attacken besitzen das Potenzial, die zum Opfer gewordenen Firmen nachhaltig zu schädigen und sogar in ihrer Existenz zu gefährden.

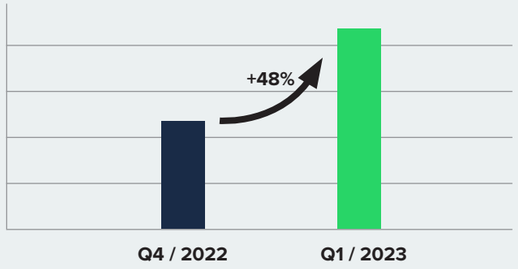
Cyber-Risiko DDoS: Die Bedrohungslage für Schweizer Unternehmen wächst

Cyber-Attacken von Kriminellen können jedes Unternehmen unabhängig von dessen Grösse und Branche treffen. In einigen Teilen Europas hat bereits jedes zweite (!) Unternehmen eine solche Attacke erlebt. Mit beträchtlichen Folgen: Wie der Branchenverband Bitkom für Deutschland errechnet hat, verursachten die Angriffe einen Schaden von 203 Mrd. Euro.

DDoS-Attacken (Distributed Denial of Service) gehören hier zu den häufigsten Delikten. Wie die aktuellen Zahlen von Link11 zeigen, sind die Angriffe im ersten Quartal 2023 im Vergleich zu Ende 2022 (Q4/2022) deutlich angestiegen (+48 %). Bei diesen Angriffen werden die Systeme der Opfer mit Anfragen regelrecht überflutet, um die gesamte Infrastruktur in die Knie zu zwingen. So war die Webseite des Kantons St. Gallen infolge der DDoS-Attacken im Sommer und Herbst 2021 wiederholt nicht erreichbar.[1] Auch die Angriffe auf das Berufsbildungszentrum SDBB im Oktober 2021 sorgten für Schlagzeilen.[2] Ein DDoS-Angriff auf den Züricher Verkehrsverbund ZVV führte im Oktober 2022 zu einem Totalausfall des ZVV-Ticketsystems[3].

Das Wachstum der Cyber-Attacken hat auch mit einer gestiegenen Verletzlichkeit der Unternehmen und Verwaltungen zu tun. Im Rahmen der Digitalisierung werden die IT-Landschaften immer komplexer. Verschiedene Cloud-Typen (Public, Private, Hybrid) treffen auf virtualisierte Maschinen, in denen Mikroservices und Open-Source-Elemente miteinander interagieren. Dazu kommt

Entwicklung DDoS Attacken Q4/2022 – Q1/2023



eine gestiegene Zahl an Netzwerkkomponenten, die mit dem Firmennetzwerk kommunizieren muss. Hier sind mobile Devices der Mitarbeitenden, aber auch Sensoren und Aktoren des Internet der Dinge (IoT) zu nennen. Aufgrund der Verzahnung digitaler Wertschöpfungsketten spielen auch Application Programming Interfaces (APIs) eine immer grössere Rolle und werden zum Flaschenhals. APIs sind lastempfindlich. Auch kleine DDoS-Angriffe können dadurch bereits für einen Dominoeffekt in der Wertschöpfungskette sorgen und diese zum Erliegen bringen.

Demgegenüber lässt sich eine stärkere Professionalisierung der Kriminellen beobachten, welche die Effizienz und Effektivität ihrer Angriffsmethoden weiter steigern.

Die Komplexität von DDoS-Attacken steigt deutlich. So wächst die Zahl der Multivektor-DDoS-Angriffe, bei denen verschiedene technische Schwachstellen auf Transport-, Applikations- und Protokollebene gleichzeitig attackiert werden (z. B. UDP, TCP). Sogenannte Reflection-Amplification-Attacken nutzen unzureichend konfigurierte Dienste und Server aus. Sie sind indirekte Multivektor-Attacken. Zunächst werden missbräuchliche Datenpakete nur in begrenztem Umfang übertragen, dann aber vielfach verstärkt an das eigentliche Ziel weitergeleitet.

Die Angreifer steigern zudem die Effektivität der Attacken, indem sie sich selbst der Cloud bedienen. Dazu nutzen sie die Kapazitäten der Hyperscaler (AWS, Google Cloud usw.) aus. Inzwischen werden 40 bis 45 Prozent aller Attacken über diese Wege ausgeführt. Den Angreifern gelingt es hier, Schwachstellen der Server-Instanzen auszunutzen bzw. unzureichend geschützte APIs zu kompromittieren, um so die Infrastruktur für eigene Angriffe zu benutzen. Das Versprechen nahezu unbegrenzter Skalierbarkeit, das die Cloud macht, nutzen eben auch Kriminelle.

Ransomware, CEO-Fraud und andere Straftaten setzen Firmen zu

DDoS-Attacken gehören zwar zu den Cyber-Attacken mit dem grössten Wachstum. Sie sind aber längst nicht die einzige Bedrohung, der Unternehmen ausgesetzt werden. Vielfach kombinieren die Angreifer DDoS-Attacken mit anderen Formen von Cyber-Crime bzw. versuchen, die Aufmerksamkeit der IT-Teams mit gezielten Überlastungsangriffen auf sich zu ziehen, um etwa Daten zu stehlen. Erst im Januar 2022 tauchten in einem Hackerforum 3,7 Millionen Kundendaten eines digitalen Kalenderdienstes auf. Ein DDoS-Angriff auf die Cloud-Server des Unternehmens wird mit dem Ableiten der Daten in Verbindung gebracht.[4]

Darüber hinaus haben in den vergangenen Jahren Erpressungsversuche mit Ransomware stark zugenommen. Dabei schleusen die Kriminellen (teilweise auch als Folge von DDoS-Attacken) Schadsoftware in das Unternehmensnetzwerk ein. Durch den erfolgreichen DDoS-Angriff werden z.B. Webserver zum Neustarten gezwungen, wodurch die Ereignisse ihren Lauf nehmen und Schadsoftware in Umlauf kommt. Diese verschlüsselt dann die hier gespeicherten Daten. Um wieder mit den Systemen arbeiten zu können, werden die Opfer zur Zahlung eines Lösegelds aufgefordert. Anders als bei klassischen Erpressungsversuchen gehen die Täter bei der „Übergabe“ des Lösegelds wenig Risiko ein. Sie erwarten die Zahlungen vorzugsweise in Bitcoin; und damit anonym. Zum Teil treten parallel abermals DDoS-Angriffe in Erscheinung, um den Lösegeldforderungen Nachdruck zu verleihen.

Auch hier zeigen die Täter hohe Professionalität und suchen sich ihre Opfer gezielt aus, um möglichst hohe Beute zu machen. Gerade Handelsunternehmen sind in den vergangenen Monaten häufiger Opfer s olcher Angriffe geworden. Zuletzt etwa die bekannte Elektronikkette MediaMarkt-Saturn aus Deutschland.[5]

Im Sommer 2022 hat die Agentur der Europäischen Union für Cybersicherheit (European Network and Information Security Agency = ENISA) die zehnte Ausgabe ihres jährlichen Reports «ENISA Threat Landscape 2022» vorgestellt. Darin fasst sie die aus ihrer Sicht wichtigsten aktuellen Bedrohungen zusammen. Über DDoS-Attacken hinaus listet sie darin u. a. auf:

- Ransomware und Malware
- Social Engineering-Bedrohungen
- Bedrohungen der Verfügbarkeit und Integrität von Informationen
- Desinformation
- Angriffe auf die Supply-Chain

Jeder Angriff hat das Potenzial, das Unternehmen dauerhaft zu schädigen. Zu den direkten finanziellen Auswirkungen, die aus dem Stillstand von Systemen erwachsen (Umsatzverluste, Konventionalstrafen, weil Termine nicht eingehalten werden können, oder Lösegeld), kommen indirekte Schäden hinzu, die aus dem Reputationsverlust und dem erschütterten Vertrauen auf Seite der Kunden erwachsen.

Regulatorische Vorschriften bergen ebenfalls Risiken

Indirekt ergeben sich aus dem Treiben Krimineller auch Risiken durch regulatorische Vorschriften. In diesem Zusammenhang ist vor allem das totalrevidierte schweizerische Datenschutzgesetz zu nennen, das etliche neue Vorgaben für schweizerische Unternehmen bringen und ohne Übergangsfristen auf den 1. September 2023 in Kraft treten wird.

Im Bereich der Datensicherheit stellt das neue Datenschutzgesetz folgende Anforderungen auf:

Unternehmen müssen angemessene technische und organisatorische Massnahmen implementieren, um eine dem Risiko angemessene Datensicherheit zu gewährleisten. Mit solchen Massnahmen soll sichergestellt werden, dass die stetige Vertraulichkeit, Integrität und Verfügbarkeit von Personendaten bestmöglich gewährleistet sind. Welche technischen und organisatorischen Massnahmen angemessen sind, hängt vom Zusammenspiel zwischen dem Risiko für die betroffenen Personen und der Eintretenswahrscheinlichkeit einer Datensicherheitsverletzung ab. Grundsätzlich gilt, je sensitiver und umfangreicher die von einem Unternehmen bearbeiteten Personendaten sind, desto grösser ist das Risiko für die betroffenen Personen und desto höher sind die Anforderungen an angemessene Datensicherheitsmassnahmen. Zur Eintretenswahrscheinlichkeit von Datensicherheitsverletzungen als zweiter Faktor ist anzumerken, dass dieser aufgrund der enormen Zunahme von Cyber- Attacken in den letzten Jahren ebenfalls gestiegen ist. Das revidierte Datenschutzgesetz verlangt nicht nur die Implementierung angemessener technischer und organisatorischer Massnahmen, sondern auch deren Überprüfung und Validierung in regelmässigen Abständen.

Bei der Einführung neuer Personendatenbearbeitungen, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen, müssen Schweizer Unternehmen neu im Voraus eine sog. Datenschutz-Folgenabschätzung durchführen. Im Rahmen der Datenschutz-Folgenabschätzung muss (i) die geplante Bearbeitung beschrieben, (ii) eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person vorgenommen sowie (iii) die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte dargestellt werden. Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Personendatenbearbeitung trotz der vorgesehenen Massnahmen noch immer ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat, müssen Unternehmen vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB vorgängig eine Stellungnahme zur Bearbeitung einholen.

Das revidierte schweizerische Datenschutzgesetz übernimmt aus der europäischen Datenschutzgrundverordnung («DSGVO») die Grundsätze von «Privacy by Design» und «Privacy by Default». Insbesondere mit dem Grundsatz von «Privacy by Design» soll sichergestellt werden, dass Datensicherheit bereits bei der Entwicklungvon Soft- und Hardware oder beim Einkauf bzw. der Lizenzierung solcher Produkte berücksichtigt wird. Unternehmen sollten daher beim Entscheid über den Einsatz neuer Soft- oder Hardware auch prüfen, ob diese Produkte über eine angemessene, dem Stand der Technik entsprechende Datensicherheit verfügen.

§ Mit dem revidierten Datenschutzgesetz werden neue Meldepflichten bei Datensicherheitsverletzungen (z.B. bei Cyber-Security-Attacken) eingeführt, die das schweizerische Recht bislang so nicht kannte. Unternehmen müssen neu dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten («EDÖB») Datensicherheitsverletzungen so rasch wie möglich melden, sofern diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person(en) führen. Wann ein solches hohes Risiko vorliegt, ist eine Rechtsfrage, bei welcher Unternehmen einen gewissen Auslegungsspielraum haben. Zudem müssen Unternehmen neben der Meldung an den EDÖB auch die von der Datensicherheitsverletzung betroffenen Personen informieren, wenn es zu deren Schutz erforderlich ist oder der EDÖB es verlangt. Bislang konnten schweizerische Unternehmen Cyber-Attacken oder andere Datensicherheitsverletzungen diskret behandeln; neu werden sie aufgrund dieser Meldepflichten aber womöglich gezwungen sein, die Vorfälle publik zu machen.

Anders als im bisherigen Recht drohen bei der vorsätzlichen Verletzung (worunter auch das Inkaufnehmen fällt) der Datensicherheit nicht nur zivilrechtliche Haftungsklagen, sondern gar strafrechtliche Sanktionen mit Bussen von bis zu CHF 250’000.00. Als schweizerische Eigenheit handelt es sich bei diesen Bussen nicht um Unternehmensbussen, sondern um strafrechtliche Sanktionen, die ad personam gegen die für die Datenschutzverletzung verantwortliche Person gerichtet sind. Da es sich beim Thema Datensicherheit aufgrund dessen hohen operationellen Relevanz für Unternehmen um eine Aufgabe handelt, die auf Stufe des Verwaltungsrats oder der Geschäftsführung angesiedelt werden muss, bestehen bei der Verletzung der datenschutzrechtlichen Vorgaben zur Datensicherheit insbesondere für Verwaltungsrats- und Geschäftsführungsmitglieder erhebliche strafrechtliche Risiken.

Cyberversicherungen: Nicht in falscher Sicherheit wiegen

In den vergangenen Jahren haben Cyber-Versicherungen einen regelrechten Boom erlebt. Fast alle grossen und kleinen Versicherer haben Policen entwickelt, mit denen sich Unternehmen gegen die finanziellen Risiken von Cyber-Attacken versichern können. Unternehmen dürfen sich aber nicht in falscher Sicherheit wiegen. Denn die gewaltige Zunahme von erfolgreichen Ransomware-Attacken und den damit verbundenen Lösegeldzahlungen führen dazu, dass sich erste Versicherer aus diesem Geschäft wieder zurückziehen. Die Schadensquoten sind zu hoch und der Vertrag lohnt sich für die Versicherung nicht. Die AXA etwa wird in ihrem Stammmarkt keine Lösegelder mehr zahlen.[6] Auch das Versicherungsunternehmen Lloyds of London schränkt den Leistungsumfang seiner Cyber-Policen ein, indem man Ausschlussklauseln zu «Cyber War and Cyber Operations» erlässt.[7] Der Schutzschirm, den eine Versicherung verspricht, wird also löchrig. Zudem dürfen die bereits erwähnten Schäden bei Reputation und Regulatorik nicht vergessen werden. In dieser Hinsicht bieten Versicherungen ohnehin kaum Schutz.

Unternehmen brauchen jetzt eine Sicherheitsstrategie

Eine sich verschärfende Bedrohungslage, geringere Unterstützung durch Versicherungen und gleichzeitig mehr Druck durch regulatorische Vorschriften: Unternehmen müssen jetzt handeln und Massnahmen ergreifen. Cyber-Sicherheit muss zur Chefsache werden.

Dabei ergeben sich drei Handlungsfelder

1 Jeder erfolgreiche Angriff, der trotz aller Massnahmen durchaus denkbar ist, führt im schlimmsten Fall zum Stillstand in Teilen eines Unternehmens. Es muss ein Business Continuity Management entwickelt werden, das sich im Sinne einer Notfallplanung damit beschäftigt, wie schnell ein Unternehmen wieder handlungsfähig ist. Und dabei auch den Wiederanlauf von wiederhergestellten Systemen berücksichtigt und koordiniert.

2 Aus juristischer Sicht sind vor allem folgende Massnahmen mit hoher Priorität zu empfehlen:

- Unternehmen müssen risikobasiert überprüfen, ob sie angemessene technische und organisatorische Massnahmen getroffen haben, um eine ausreichende Datensicherheit zu gewährleisten. Hierfür ist es durchaus zu empfehlen, sich an Beratungsunternehmen zu wenden.
- Die neuen Meldepflichten bei Datensicherheitsverletzungen erfordern, dass in sehr kurzer Zeit die Risiken eines Cyber-Security-Incidents aus juristischer und fachlicher Perspektive beurteilt werden und damit verbunden entschieden wird, ob der EDÖB oder die betroffenen Personen informiert werden müssen. Eine entsprechende Meldekette kann im Rahmen der Notfallplanung eines Business Continuity Management integriert werden.
- Unternehmen sollten interne Prozesse für die Erstellung von Datenschutz-Folgeabschätzungen implementieren.
- Beim Entscheid über den Einkauf neuer Soft- und Hardware ist zu prüfen, ob diese Produkte über eine ausreichende Datensicherheit verfügen.
- Zudem sollten Unternehmen auch die Umsetzung aller übrigen neuen Vorgaben beachten, die das revidierte schweizerische Datenschutzgesetz statuiert (z.B. erweitere Informationspflicht bei der Beschaffung von Personendaten, Abschluss von Auftragsbearbeitungsvereinbarungen beim Outsourcing von Personendatenbearbeitungen, Ergreifen von Schutzmassnahmen bei der Bekanntgabe von Personendaten ins Ausland etc.).

3 Schliesslich sind technische Massnahmen zu ergreifen, um die eingesetzten Systeme und die Infrastruktur zu schützen. Da DDoS-Attacken zu den grössten Bedrohungen gehören, sollte ihnen auch eine hohe Priorität eingeräumt werden.

Technische Massnahmen gegen DDoS

DDoS-Angriffe sind rein konzeptionell der sprichwörtliche «alte Hut» in der IT. Zur Abwehr solcher Attacken nutzen viele Unternehmen und Carrier- und hardware-basierte Systeme. Viel zu oft verlassen sich Firmen allerdings darauf, dass ihr Hosting- und Zugangsprovider die notwendige Technik betreibt.

Dieser «Schutz» genügt angesichts der neuen Dimensionen in der Bedrohung aber nicht mehr. Zum einen gehören DDoS-Abwehrmassnahmen nicht unbedingt zur Kernkompetenz der Dienstleister. Durch falsch dimensionierte oder unzureichend konfigurierte Standard-Lösungen ergeben sich damit Schwachstellen. Zudem sollte im Sinne der Regulatorik nicht vergessen werden, dass Unternehmen für die Datensicherheit von personenbezogenen Daten verantwortlich bleiben, auch wenn sie sich eines Dienstleisters bedienen.

Nimmt der Angriff zu viel Zeit oder Ressourcen des Carriers in Anspruch, so behält sich dieser häufig das «Null-Routing» vor. Das bedeutet, ein komplettes Abschalten des Datenverkehrs über einen nicht kalkulierbaren Zeitraum – ggf. auch über Stunden und Tage hinweg. Zu Bedenken ist auch, dass der Carrier selbst in das Visier von Angreifern geraten kann. Unternehmen werden damit indirekt zu Opfern.

Einen grösseren Einfluss haben Unternehmen durch den Einsatz lokaler Hardware im eigenen Rechenzentrum vor Ort. Dabei darf aber der damit verbundene Aufwand nicht unterschätzt werden. Aufgrund der zunehmenden Angriffsgrösse skalieren hardware-basierte Ansätze oftmals nicht mehr und sind wirtschaftlich ineffizient. Entweder ist die Umgebung kostspielig überdimensioniert, sodass sie kaum Auslastung erfährt und Leerstandskosten produziert. Oder aber – und dies ist in der Praxis noch viel wahrscheinlicher – sie ist neuralgisch unterdimensioniert und kann bereits einem mittelgrossen Angriff nicht ansatzweise die Stirn bieten. Hinzu kommt, dass diese Modelle statisch und regelbasiert sind und damit nicht dynamisch auf neue Angriffstechniken vorbereitet sind. Im Ergebnis unterwandern diese den Schutz und der Schaden tritt ein. Zudem sind viele Verfahren reaktiver Natur und basieren auf dem Faktor Mensch. Erst wenn ein Angriff festgestellt wird, dann wird Datenverkehr umgelenkt und versucht, diesen abzuwehren. Allein bis zur Erkennung und bis zum erfolgreichen Umlenken des Datenverkehrs vergeht kostbare Zeit. Die Entstörung bindet Ressourcen und der Ausfall zieht sich mitunter über viele Stunden in die Länge. Im Zeitalter der Digitalwirtschaft sind diese Ansätze heute schlichtweg nicht mehr zeitgemäss. Das Ausweichen auf Tunneling ist nur vorderhand ein adäquater Schutz. Bei grossen Datenmengen weist es viel zu starke Begrenzungen auf.

Es bietet keine ausreichende Fehlerkorrektur, leidet unter instabiler Latenz und ist verlustanfällig. Auch niedrige Durchsatzraten und die Overhead-Zusatzlast durch das Tunneling sind Nachteile.

Eine zeitgemässe Antwort auf DDoS-Attacken liegt dort, wo sie in der Regel ihren Ursprung haben: Cloudbasierte Dienste wie von Link11 erlauben es Unternehmen, den Angreifern auf Augenhöhe zu begegnen.

Die moderne Technologie setzt auf den Ansatz von «Whitelisting». Hier konzentriert man sich auf das Profiling des legitimen Datenverkehrs. In Anlehnung an das Prinzip «Zero Trust» werden jedwede Anomalien sofort erkannt und überprüft bzw. blockiert. Es gilt für den Netzwerkverkehr also eine Art von «Beweislastumkehr».

Gegenüber der klassischen und auf Regeln basierenden Filtern, die von Unternehmen auf eigener Hardware gewählt werden, verlaufen die Analysen automatisiert und nutzen Methoden der KI wie das «Machine Learning». Es kommt keine klassische Pattern-Erkennung zum Einsatz, sondern eine automatisierte Realtime-Analyse von Anomalien im Traffic (Quellen, Pakete). Vorteil: Die Abwehr läuft auf dieser Grundlage wesentlich schneller und präziser.

Der cloudbasierte Ansatz bringt noch einen weiteren grossen Vorteil mit sich. Die Lösung ist problemlos skalierbar und erlaubt eine Behebung von Problemen in Echtzeit. Zeitaufwendige Ansätze von «Patch/Fix» entfallen. Schutz aus der Cloud ist redundant. Ein wichtiger Aspekt bei Überlastungsangriffen. Dank zentraler Reputation-Datenbank profitieren die Kunden zudem von einem Sofort-Schutz. Tritt irgendwo im weltweiten Netz eine neue Bedrohung auf, wird diese in Echtzeit in der zentralen Datenbank automatisch erfasst und auf alle Standorte gespiegelt. Alle Kunden sind weltweit binnen Sekunden gewappnet, ohne dass jemand Hand anlegen muss.

Ihre IT-Sicherheitslösung für die Zukunft

Die Bedrohungslandschaft für Schweizer Unternehmen wird immer dynamischer. Die Zahl der Angriffe und deren Wucht wachsen stark. Zudem nimmt der regulatorische Druck zu. In diesem herausfordernden Umfeld bieten zeitgemäße Schutzlösungen wie die cloudbasierten Dienste von Link11 das langfristig notwendige Schutzlevel. Für einen ganzheitlichen Schutz der unternehmenseigenen IT-Infrastrukturen und kritischen Anwendungen und zur Stärkung der Cyber-Resilienz setzt Link11 mit seiner integrierten Cloud Security Plattform auf künstliche Intelligenz, maschinelles Lernen, Automatisierung und Echtzeit-Abwehr. Wenn Sie wissen möchten, wie Sie unter Einhaltung der europäischen Rechtsnormen Ihre IT-Infrastruktur, Netzwerke und Applikationen gegen Cyber-Attacken schützen können, stehen wir Ihnen Rede und Antwort. Haben Sie dagegen Fragen zu den regulatorischen Vorgaben, insbesondere im Rahmen des totalrevidierten schweizerischen Datenschutzgesetzes, so steht Ihnen die Anwaltskanzlei bratschi jederzeit gerne zur Verfügung. Bratschi berät aktuell eine Vielzahl von Unternehmen aus ganz verschiedenen Branchen bei der Implementierung der Vorgaben des neuen schweizerischen Datenschutzgesetzes und steht Ihnen für Fragen zu diesem Bereich jederzeit gerne zur Verfügung.

Ihr Ansprechpartner für juristische Fragen zum Thema Datenschutz:

Dr. Adrian Bieri
Bratschi AG, Rechtsanwalt / Partner
Adrian.Bieri@bratschi.ch
+41 58 258 10 00

Ihre Ansprechpartner für die Absicherung Ihrer IT-Infrastrukturen:

Jürgen Schreiner
Link11, Account Executive
sales@link11.com
+49 69 264929777

Jonas Jansen
Link11, Head of Channel Sales
sales@link11.com
+49 69 264929777

Nachweise

[1] https://www.srf.ch/news/schweiz/ddos-attacken-gehackte-st-galler-kantonswebsite-es-geht-nicht-nur-um-geld

[2] https://www.inside-it.ch/de/post/heftiger-ddos-angriff-auf-berufsbildungszentrum-sdbb-20211008

[3] https://www.watson.ch/schweiz/mobilit%c3%a4t/437771637-zvv-hackerangrff-legt-alle-ticketkanaele-lahm

[4] https://www.cpomagazine.com/cyber-security/3-7-million-flexbooker-accounts-leaked-to-hacker-forum-after-ddos-attack/

[5] https://t3n.de/news/mediamarkt-saturn-angriff-loesegeld-1425771

[6] https://www.heise.de/news/Cyber-Versicherungen-Axa-will-kein-Ransomware-Loesegeld-mehr-zahlen-6045237.html

[7] https://threatpost.com/lloyds-cyber-insurance-exclusions/176669/

Hauptsitz

Link11
Lindleystr. 12
60314 Frankfurt