IONOS

IT-Security in der Cloud neu definiert

Komplexe Netzwerkangriffe zuverlässig verhindern

IONOS

Inhalt

1 Digitalisierung und IT-Security im Cloud-Zeitalter

Service-Ausfall und digitale Erpressung effektiv stoppen

Mit der fortschreitenden Digitalisierung unseres Lebens wachsen die Gefahren, dass Systeme und Geräte angegriffen werden. Dabei gewinnen beispielsweise die neuen Internet of Things (IoT)-Technologien stark an Bedeutung, denn sie vernetzen unzählige Geräte, die wir jeden Tag im Haushalt verwenden oder die beispielsweise in Maschinen und Sensoren überall auf der Welt zum Einsatz kommen. Obwohl das IoT entwickelt wurde, um unseren Alltag zu vereinfachen und zu bereichern, werden Systeme durch ihre immer weiter reichenden Netzwerkverbindungen vermehrt zum Ziel von Angriffen. Mittlerweile verursachen Attacken auf IT-Systeme in aller Welt wirtschaftliche Schäden in Milliardenhöhe.[1] Dabei ist das kriminelle Potenzial so enorm, dass Viren, Trojaner und Malware, aber auch komplexere Ransomware- und Distributed Denial of Service (DDoS)-Angriffe existenzbedrohend werden. Sie können ohne Vorwarnung auftreten und ganze Unternehmen lahmlegen. Somit gewinnt nachhaltige und professionelle IT-Sicherheit nicht nur an Bedeutung, sondern gilt mittlerweile sogar als eine der größten Herausforderungen für die Wirtschaft und das Leben der Zukunft – auch in Deutschland. Hinzu kommt, dass Verwaltungen der öffentlichen Hand Investitionen und Modernisierungen oftmals sehr lange hinauszögern und allein aufgrund der veralteten Technik besonders angreifbar sind.

So wurden in der ersten Hälfte des Jahres 2021 weltweit 5,4 Millionen DDoS-Attacken gezählt.[2] Und auch im Bereich der Ransomware steigt die Zahl der Angriffe dramatisch an. Der Global Risks Report des World Economic Forums aus dem Jahr 2019 verzeichnet eine Steigerung der Ransomware-Angriffe um 97 Prozent innerhalb von zwei Jahren.

Diesen Entwicklungen versuchen Security-Anbieter mit ständig neuen Sicherheitslösungen Herr zu werden, denn nur so können Unternehmen und Einrichtungen ihre IT schützen. Über Jahrzehnte hinweg sind die Sicherheitslösungen besser und komplexer geworden, doch auch die Bedrohungen durch die Hacker werden immer raffinierter. Daher haben Security-Spezialisten nun auch cloudbasierte Technologien entwickelt, mit denen sie Unternehmen und Einrichtungen vor den Gefahren in vernetzten Systemen zuverlässig vor DDoS-Attacken und Ransomware schützen möchten. Mithilfe von modernen Cloud-Technologien lässt sich ein besonders hoher Schutz realisieren, den vor allem kleine und mittlere Unternehmen (KMU) bzw. Institutionen nicht selbst realisieren können. Dafür fehlen ihnen in der Regel die Ressourcen und das erforderliche Know-how. Aber auch Einrichtungen der öffentlichen Hand

1. NETSCOUT (2022): NETSCOUT THREAT INTELLIGENCE REPORT, online verfügbar unter: https://www.netscout.com/threatreport.
2. NETSCOUT (2022): NETSCOUT THREAT INTELLIGENCE REPORT, online verfügbar unter: https://www.netscout.com/threatreport.

können von der Cloud Security profitieren, denn mit einer modernen SaaS-Architektur und dem richtigen Partner stellen sie die Sicherheit und Souveränität ihrer Daten sicher. Doch was bedeuten eigentlich DDoS und Ransomware im Detail und welche Gefahren sind damit verbunden?

2 Definition der Begriffe – Worüber reden wir eigentlich?

2.1 Denial of Service (DoS)

‚Denial' ist das englische Wort für ‚Verweigerung' und somit bezeichnet schon der Begriff ‚Denial of Service' (DoS) den Kern des Problems. Mit einem DoS-Angriff werden Netzwerkressourcen vorsätzlich eingeschränkt – beispielsweise aus politischen Gründen oder Im Sinne einer gezielten Erpressung. Ziel dieses Angriffs ist es, einem Unternehmen oder einer Einrichtung durch die massive Störung von alltäglichen Prozessen einen möglichst großen Schaden zuzufügen. Dazu nutzen Kriminelle spezielle DoS-Software, die zahlreiche Anfragen an eine ausgewählte Webressource sendet. Hierdurch wird der Internet-Traffic so massiv gesteigert, dass etwa die Website eines Unternehmens nicht mehr schnell genug reagieren kann oder komplett ausfällt. In anderen Fällen wird Mitarbeitern der Zugriff auf ihre E-Mails verwehrt oder Applikationen laufen so langsam, dass sie praktisch nicht mehr nutzbar sind. Hiervon sind vor allem Online Shops, Anbieter von Online Services und Einrichtungen, deren Erfolg von einem zuverlässigen Datenverkehr abhängig ist, betroffen. Angriffe auf Einrichtungen der öffentlichen Hand können ebenfalls von großer Tragweite sein, denn hier kann ein Systemausfall großen politischen oder gesellschaftlichen Schaden anrichten. Zudem arbeiten die meisten Behörden und die Mehrzahl der Unternehmen mit hochsensiblen Daten, die jederzeit zur Verfügung stehen müssen.

Tatsächlich kann ein DoS-Angriff jede Infrastruktur betreffen, die Daten mit dem Internet austauscht – von der vernetzten Fertigungsanlage, über ein Rechenzentrum, bis hin zu einzelnen Webseiten. Somit sind die Gefahren von DoS fast schon grenzenlos, denn in unserer modernen, digitalisierten Welt wird der Erfolg in Wirtschaft und Gesellschaft von Technologien bestimmt. Fallen diese aus, sind Unternehmen, Einrichtungen, Behörden oder Personen plötzlich nicht mehr erreichbar oder nur eingeschränkt arbeitsfähig.

Ein DoS-Angriff kann jede Infrastruktur treffen, die Daten mit dem Internet austauscht.

Aber damit nicht genug, denn die klassischen DoS-Attacken werden mittlerweile von den sogenannten DDoS-Angriffen abgelöst. Deren Potenzial ist um ein Vielfaches größer. Bei einem DDoS-Angriff handelt es sich um eine verteilte Netzwerkattacke, die über mehrere Rechner oder Geräte gleichzeitig ausgeführt wird. Bei dieser Strategie kapern Angreifer unzählige Systeme oder Maschinen sowie Server und PCs – bis hin zu Smartphones und kleinen IoT-Geräten, um sie im Verborgenen zu vernetzen und zu kontrollieren. So wird jedes infizierte Gerät zu einem sogenannten ‚Bot' bzw. ‚Zombie', ohne dass es

deren Nutzer überhaupt merken. Die Bots verbreiten den DoS-Virus dann selbständig weiter und infizieren weitere Geräte. Mithilfe einer Malware werden diese Connected Devices dann vom Angreifer über einen sogenannten Botnet-Command-and-Control-Server ferngesteuert und bei Bedarf gleichzeitig aktiviert. Somit ist es leicht nachvollziehbar, dass der Angriff einer großen Bot-Armee, die aus mehreren Tausend Einheiten bestehen kann, massive Schäden anrichtet. Aber damit ist es nicht genug, denn mittlerweile haben Kriminelle ihre Technologien nochmals weiterentwickelt und sind nunmehr dazu in der Lage, illegale Bot Services nach individuellen Vorgaben eines einzelnen Hackers für ein bestimmtes Ziel als gemietete Ransomware-as-a-Service (RaaS)-Dienstleistung anzubieten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht in einem Bericht aus dem Jahr 2021 daher auch von Cybercrime-as-a-Service (CCaaS).

2.2 Ransomware

Ein Ransomware-Angriff ähnelt vom Grundsatz her einer DoS-Attacke, denn auch hier hindert eine spezielle Schadsoftware bestimmte Nutzer vorübergehend oder dauerhaft daran, auf ihre eigenen Systeme zuzugreifen. Seinem Namen nach dient ein Ransomware-Angriff der Erpressung von Lösegeld. Hierfür werden sensible Daten verschlüsselt oder sogar komplett gestohlen, um diese dann zu verkaufen bzw. mit einer Veröffentlichung zu drohen (typisches Beispiel: Hive-Ransomware), wenn das Opfer den Forderungen des Angreifers nicht nachkommt.

Doch soweit muss es in der Praxis nicht einmal kommen, denn allein die Sperrung eines Systems oder der ‚Verlust' von Daten können massiven wirtschaftlichen Schaden anrichten – etwa durch die Unterbrechung von Lieferketten

oder Kommunikationswegen. Ransomware-Attacken treffen oft KMU bzw. Einrichtungen, denn deren Systeme sind oft weniger gut geschützt und somit leichter anzugreifen. Die öffentliche Verwaltung bleibt auch nicht vor Ransomware verschont. Hier sind Daten hochsensibel und somit für Kriminelle besonders interessant.

So gelangt Ransomware ähnlich wie die klassischen Computerviren in alltäglichen Prozessen auf die anvisierten Rechner. Das können gefälschte E-Mail-Dateianhänge mit echt erscheinenden Rechnungen, Lieferscheinen oder ZIP-Dateien sein. Aber auch Sicherheitslücken in der Standardsoftware, im Webbrowser sowie bei Filehosting-Diensten wie Dropbox oder Google Drive sind für die Angreifer oftmals leichtes Spiel. Dies bestätigt auch das renommierte Analystenhaus Gartner, das in einem Bericht aus dem Jahr 2021 zusätzlich darauf hinweist, dass Ransomware immer häufiger auch als „Bestandteil eines noch umfassenderen Angriffs eingesetzt wird, der darauf abzielt, kritische Systeme und Administrationsfunktionen zu kompromittieren."

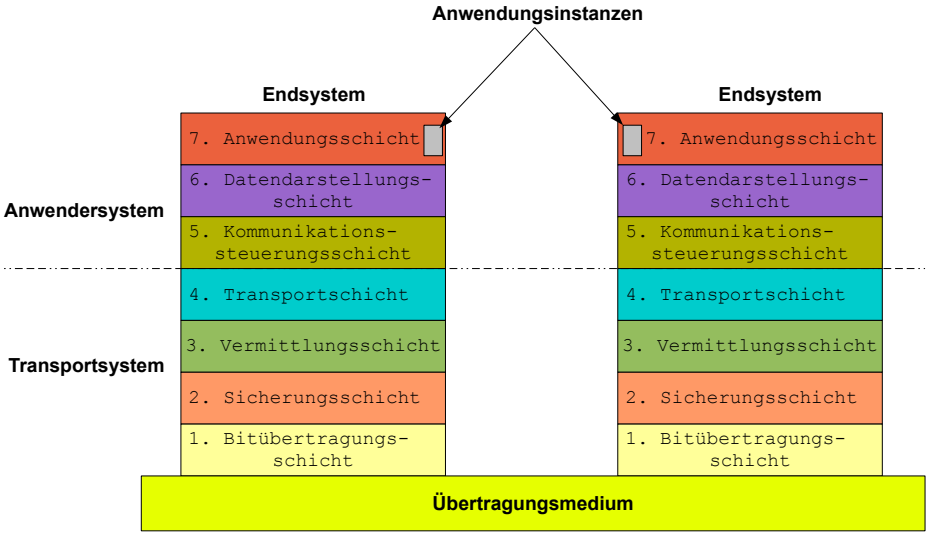
Angesichts der wachsenden Gefahren durch DoS- und Ransomware-Attacken sollte der zuverlässige Schutz vor diesen Angriffen (Resilience) zur Grundausstattung jedes Unternehmens und jeder Einrichtung gehören – unabhängig von Größe, Branche oder Region.

3 Reale Gefahren – Wo manifestieren sich Bedrohungen?

3.1 Arten von Angriffen

Ein zuverlässiger Schutz ließe sich leicht etablieren, wenn die Angriffe klar umrissen wären und einem immer gleichen Muster folgen würden. Doch leider ist das nicht der Fall. Gerade bei den DDoS-Attacken nutzen sie in der Regel mehrere Varianten gleichzeitig, um ihre kriminellen Ziele zu erreichen. Die Angriffsarten korrespondieren in großen Teilen mit den einzelnen Schichten des sog. ‚Open System Interconnection-Modells' (OSI-Modell), das in der nachfolgenden Abbildung zusammengefasst wurde. Dieses mehrschichtige Framework gilt weithin als Design-Grundlage für herstellerunabhängige Kommunikationsstandards. Es unterscheidet insgesamt sieben Schichten (sog. Layers), wobei jede Schicht eine eigene Aufgabe hat. Das Modell ist hierarchisch aufgebaut, das heißt jede Schicht greift über eine Schnittstelle auf die jeweils darunter liegende zu, um dem übergeordneten Layer Dienste zur Verfügung zu stellen. Neben dem verbreiteten OSI-Modell unterscheiden Experten auch in volumetrische DDoS-Angriffe, Protokoll-Attacken (sog. ‚Flooding' wie z.B. SYN-Floods und Smurf-DDoS) und Angriffe auf der Anwendungsebene (u.a. Ping of Death- und LAND-Attacken).

Da die Angriffe nicht klar umrissen sind und keinem immer gleichen Muster folgen, lässt sich auch kein zuverlässiger Schutz etablieren.



ISO-OSI-7-Schichten-Modell (Quelle: Wikipedia)

Die sieben Schichten des OSI-Modells

- Obere (anwendungsorientierte) Schichten
  - Schicht 7 / Application Layer
    Diese Schicht stellt den direkten Kontakt zum Anwender her. Hier erhalten E-Mail-Programme, Webbrowser und andere Applikationen ihre Zusatzinformationen. Dieser Prozess wird auch auch Kapselung genannt.
  - Schicht 6 / Presentation Layer
    Auf dieser Ebene werden lokale Darstellungen in standardisierte Formate überführt. Dabei wird z.B. festgelegt, wie eine E-Mail-Nachricht dargestellt werden soll – inklusive ihrer zugehörigen Dateiformate (z.B. jpg, MPEG4 o.ä.) und der Art der Komprimierung.
  - Schicht 5 / Session Layer
    Der Session Layer wird auch als Kommunikationsschicht bezeichnet. Mit speziellen Steuerungs- und Kontrollmechanismen wird hier eine Verbindung zwischen den oberen Schichten hergestellt und geregelt.

- Untere (transportorientierte) Schichten
  - Schicht 4 / Transport Layer
    Die Transportschicht ist das zentrale Bindeglied zwischen den anwendungsorientierten und den transportorientierten Schichten. Auf diesem Übertragungskanal wird eine logische Ende-zu-Ende-Verbindung zwischen den kommunizierenden Systemen hergestellt. Zudem erhält das Datenpaket, das in den anwendungsorientierten Schichten um einen speziellen Header erweitert wurde, hier noch einen zusätzlichen Transport-Header. Ebenso erfolgt die Zuordnung eines Datenpakets zu einer bestimmten Anwendung.

- Schicht 3 / Network Layer
  Auf dieser Vermittlungsschicht erreicht die Datenübertragung das Internet und eine logische Adressierung der Endgeräte inklusive Zuordnung von eindeutigen IP-Adressen wird vorgenommen. Das Datenpaket erhält hier einen Network-Header mit Informationen zum Routing und zur Datenflusskontrolle. Dafür werden Standards wie IP, ICMP, X.25, RIP oder OSPF bzw. TCP over IP verwendet.
- Schicht 2 / Data Link Layer
  In dieser Sicherungsschicht geht es vor allem um Fehlererkennung, Fehlerbehebung und Datenflusskontrolle. So werden Übertragungsfehler weitgehend vermieden. Hierfür wird das Datenpaket inklusive Application-, Presentation-, Session-, Transport- und Network-Header von einem Frame aus Data-Link-Header und Data-Link-Trail eingerahmt. Zudem findet die Hardware-Adressierung mit sogenannten MAC-Adressen statt. Der Zugriff aufs Medium wird durch Protokolle wie Ethernet oder PPP geregelt.
- Schicht 1 / Physical Layer
  Diese unterste Ebene ist die Bit-Übertragungsschicht. Hier werden die einzelnen Bits eines Datenpaketes in ein physikalisches Signal umgewandelt, das über ein Medium – z.B. einen Kupferdraht, über Glasfaser oder über die Luft – übertragen werden kann. Hierfür werden Protokolle und Normen wie DSL, ISDN, Bluetooth, USB (physischer Layer) oder Ethernet (physischer Layer) eingesetzt.

Grundsätzlich gilt:
Im OSI-Modell durchlaufen die betroffenen Datenpakete jede einzelne Schicht. Das gilt ebenso für das Absendersystem wie auch für das Zielsystem. Alle anderen Geräte (z.B. ein Router), die ein Datenpaket auf dem Weg dorthin passiert, setzen lediglich an den Layers 1 bis 3 an.

In der Regel werden die Datenpakete dabei über Router transportiert. In diesem Prozess greifen die Router auf die ankommenden Informationen zu, um eine Weiterleitungsentscheidung zu treffen. Doch dafür muss ein Router das einzelne Datenpaket zunächst entpacken (sog. Entkapselung) und für die Weiterleitung später wieder neu kapseln. An dieser Stelle können IT-Security-Experten gezielt auf den Traffic zugreifen und schädliche Bestandteile eliminieren.

3.2 Welche Systeme sind besonders betroffen?

Angreifer hacken mittlerweile nicht mehr nur einzelne Computer oder Rechenzentren. Durch das IoT sind heute Milliarden internetfähige Geräte überall auf der Welt fester Bestandteil einer völlig neuen Bedrohung. Die digitalen Viren lauern nahezu überall – etwa auf dem Smartphone, im Internet-Router, in der Überwachungskamera oder sogar im digitalen Videoplayer. Selbst die smarte Beleuchtung eines Hauses kann, ohne dass es deren Besitzer überhaupt merkt, eine gefährliche Schadsoftware in sich tragen. Tatsächlich können die Netzwerkressourcen jedes beliebigen vernetzten Geräts zum stillen Teil einer Bot-Armee werden.

Doch spätestens mit dem Ausbruch der Corona-Pandemie und der damit verbundenen massiven Zunahme der Arbeit im Home Office hat sich diese ohnehin große Herausforderung noch einmal deutlich verschärft und das Thema ‚End Point Security' hat stark an Bedeutung gewonnen. Seit dem Jahr 2020 werden unzählige Notebooks, Tablets und Smartphones, die sich nicht so gut sichern und überwachen lassen wie das Innere eines Unternehmens oder ein Rechenzentrum, überall auf der Welt mit Unternehmenszentralen oder lokalen Niederlassungen verbunden. Naturgemäß birgt diese Vernetzung Schwachstellen. Auch der State of Ransomware Readyness Report, der im Jahr 2021 veröffentlicht wurde, beschäftigt sich mit diesem Thema. In der Studie von Mimecast gaben 47 Prozent der Befragten an, dass die Sicherheit ihrer Webtechnologien eine der größten Herausforderungen beim Schutz gegen die Bedrohung durch Ransomware ist – dicht gefolgt von der End Point Protection, die mit 45 Prozent ebenso deutlich ins Gewicht fällt.

Hinzu kommt die enorme Komplexität und Vielfalt der möglichen Angriffsvektoren. So verfügen zwar rund 85 Prozent der Unternehmen und Einrichtungen über erste Erfahrungen mit mindestens einer kritischen Angriffsart (ihnen wurde eine Liste mit insgesamt 17 wichtigen Herausforderungen vorgelegt), doch laut einer Studie von Osterman Research aus dem Jahr 2021 können weniger als ein Drittel der Befragten Erfahrungen mit vier oder mehr dieser sogenannten 17 Threads vorweisen. Das bedeutet, dass die meisten Unternehmen und Einrichtungen über keine praktischen Erfahrungen im Umgang mit 13 von 17 Herausforderungen verfügen. Für ein effizientes Risikomanagement ist das unzureichend. Kein Wunder, dass die meisten Befragten in der Osterman-Studie Ransomware-bezogene Themen als „bedenklich" oder „extrem bedenklich" einstufen. Immerhin gehen 61 Prozent davon aus, dass Ransomware-Attacken ihre Unternehmensdaten beschädigen würden. 59 Prozent glauben sogar, dass Ransomware-Angriffe zu einer Infektion im Bereich ihrer Endpoints führen könnten. Werden diese Zahlen um die Ergebnisse des ‚How to Prepare for Ransomware Attacks'-Reports von Gartner (November 2020) ergänzt, zeigt sich die Dramatik des Problems in besonderer Weise. Denn die Gartner-Analysten weisen darauf hin, dass die Kosten im Falle einer erfolgreichen Ransomware-Attacke weit über das in der Regel geforderte Lösegeld hinausgehen. Das ist keine Empfehlung, das Lösegeld zu zahlen, denn genau das würde das kriminelle Potenzial der Angreifer weiter fördern. Vielmehr sollten sich Anwender bei der Planung ihrer Schutzmaßnahmen bewusst sein, dass die oft mehrtägigen oder gar wochenlangen Ausfallzeiten, die Wiederherstellungskosten sowie die Reputationsschäden allein bei dieser Angriffsart 10- bis 15-mal schwerer wiegen können als das eigentliche Lösegeld. Daher ist ein vorbeugender Schutz extrem wertvoll.

85 Prozent der Unternehmen und Einrichtungen verfügen über erste Erfahrungen mit mind. einer kritischen Angriffsart.

3.3 Es kann jeden treffen – Beispiele für Attacken

Um Beispiele für DDoS-Angriffe oder Ransomware-Attacken zu finden, muss nicht lange gesucht werden. So wurde im Oktober 2021 der Automobilzulieferer Eberspächer Opfer einer Ransomware-Attacke.[3] Das Familienunternehmen aus dem baden-württembergischen Esslingen war plötzlich von der Öffentlichkeit abgeschnitten – alle Telefonverbindungen waren tagelang gekappt. Der gezielte Angriff galt den IT-Systemen.

Ein anderer Fall ereignete sich im November 2021 bei MediaMarkt Saturn. Bei dem Ingolstädter Einzelhändler verschlüsselte eine sogenannte Hive-Ransomware-Attacke das Warenwirtschaftssystem. Von einer Sekunde auf die andere waren die Kassensysteme sowie verschiedene Services in den Filialen nur noch eingeschränkt verfügbar. Nach dem gezielten Angriff dauerte es fast eine Woche, bis die Computerspezialisten des Unternehmens die betroffenen Systeme identifizieren und entstandene Schäden beheben konnten. Allein die Kosten für diesen Einsatz und der Umsatzausfall waren enorm – ganz abgesehen von der Forderung von 240 Millionen Dollar Lösegeld.[4]

Zusätzlich zu den entstandenen Schäden forderten die Angreifer 240 Millionen Dollar Lösegeld.

3. Álvarez, S. et al. (2021): Werden jetzt Heizungen und Auspuffe für Autos knapp?, online verfügbar unter: https://www.wiwo.de/technologie/digitalisierung-der-wirtschaft/nach-hackerangriff-auf-eberspaecher-werden-jetzt-heizungen-und-auspuffe-fuer-autos-knapp/27769800.html.

4. Focus Online (2021): Cyber-Attacke auf MediaMarkt und Saturn legt Systeme lahm: Mehr als 3000 Server betroffen, online verfügbar unter: https://www.focus.de/finanzen/boerse/webshops-nicht-betroffen-cyber-attacke-auf-mediamarktsaturn-legt-systeme-lahm-ueber-3000-server-betroffen_id_24407981.html.

Aber auch der öffentliche Sektor wird nicht verschont. So hat ein Verschlüsselungstrojaner im Oktober 2021 große Teile der Verwaltung der Landeshauptstadt Mecklenburg-Vorpommern in Schwerin lahmgelegt. Durch den Angriff auf einen kommunalen IT-Dienstleister mussten das komplette System heruntergefahren und alle Bürgerämter geschlossen werden. Nach Angaben des NDR war dieser Angriff kein Zufall. Vielmehr hatten die Täter eine kritische Infrastruktur im Visier und wollten gezielt an hochwertige Daten gelangen.[5] Dabei ist der Angriff auf die Verwaltung in Schwerin bei Weitem kein Einzelfall. Wie eine Umfrage vom BR und Zeit Online aus dem Jahr 2021 zeigt, wurden in den vergangenen sechs Jahren mehr als 100 IT-Systeme von Behörden, Kommunalverwaltungen und anderen staatlichen sowie öffentlichen Stellen angegriffen und verschlüsselt.[6]

4 Effizienter Schutz vor DDoS und Ransomware

4.1 Schutz als Service

Aufgrund der wachsenden Bedrohung wird der vorbeugende Schutz vor DDoS- und Ransomware-Angriffen immer wichtiger, was der zuvor genannte Osterman-Report ebenfalls klar bestätigt. Dort nennen die Befragten alle wesentlichen Schutzmaßnahmen sogar selbst:

- Multi-Factor-Authentication (78 %)
- Security Awareness Training (62 %)
- Schnelles Patchen von potenziellen Schwachstellen (64 %)
- Offsite- oder Cloud-Backup (62 %)

Keine Frage, mit diesen Maßnahmen können sich Unternehmen und Einrichtungen vor DDoS- und Ransomware-Attacken schützen, wobei Multi-Faktor-Authentifizierung und Security Awareness Trainings als grundlegende Maßnahmen auf allen Ebenen einer sicheren Netzwerkinfrastruktur realisiert werden sollten. Für das Backup hingegen existieren verschiedene Möglichkeiten, die vor allem durch die grundlegende Philosophie einer dezentralen oder zentralen (cloudbasierten) Architektur bestimmt werden. Hierbei ist in jedem Fall ein strategischer Maßnahmen-Mix von Bedeutung, wobei das Thema ‚Endpoint Security' spätestens seit der räumlichen Verlagerung von Arbeitsplätzen zunehmend in den Fokus rückt. Somit geht es heute also nicht (mehr) nur darum, ein in sich geschlossenes Unternehmensnetzwerk mit seinen klar

5. Scheller, M. (2021): Angriff auf Daten in MV: So gehen die Kriminellen vor, online verfügbar unter: https://www.ndr.de/nachrichten/mecklenburg-vorpommern/Angriff-auf-Daten-in-MV-So-gehen-die-Kriminellen-vor,itausfall110.html.

6. Zierer, M / Tanriverdi, H. (2021): Mehr als 100 Behörden erpresst, online verfügbar unter: https://www.tagesschau.de/investigativ/br-recherche/ransomware-103.html.

umrissenen Core-Technologien gegen Angriffe von außen zu schützen, sondern zunehmend auch um den rasant wachsenden Edge-Bereich (Endpoints), der unzählige lokale Geräte und Clients beim Anwender vor Ort sowie mobile Technologien beinhaltet.

An diesem Punkt können moderne Cloud-Technologien für nachhaltige Sicherheit sorgen. Die Gründe liegen auf der Hand:

Vernetzt ein Unternehmen oder eine Einrichtung die eigenen Systeme mithilfe einer zentralen Cloud, verlagert es die schützenswerten Daten und einen großen Teil des entscheidenden (d. h. angreifbaren) Traffics in ein System, das von Experten geschützt und überwacht wird. An diesem zentralen Ort lässt sich der gesamte Datenverkehr mit professionellen Security Tools rund um die Uhr kosteneffizient schützen – beispielsweise durch eine weitreichende Verschlüsselung und durch ein zuverlässiges Backup. Hinzu kommt, dass diese Aufgaben zu den Kernkompetenzen der Cloud-Anbieter gehören. Dies könnte kein Anwender vor Ort in dem Maße je realisieren.

4.2 Welche Rolle spielt die Cloud?

Vor diesem Hintergrund erstrahlt die cloudbasierte IT-Security in einem völlig neuen Licht, denn die Zahl der potenziellen Angriffspunkte verlagert sich so von einer Vielzahl nicht optimal geschützter Einzelsysteme auf eine einzige zentrale Lösung, die durch professionellen Schutz überzeugt. Das kann gerade bei komplexen DDoS- und Ransomware-Attacken für den entscheidenden Unterschied sorgen, denn in der Cloud geht es nicht mehr darum, eine Vielzahl von Geräten gegen eine große Armee von gleichgeschalteten Bots zu verteidigen, sondern den Angreifern eine gut geschützte ‚Festung' mit einem Heer von exzellent ausgebildeten ‚Soldaten' entgegen zu stellen. Somit sorgt eine cloudbasierte Security-Strategie dafür, dass die letztendlich entscheidenden Dienste auch nach einem schweren Angriff weiterhin verfügbar sind und dezentrale oder weniger wichtige Daten bei Bedarf schnell wieder hergestellt werden können.

Auch wenn an einer cloudbasierten Sicherheitsarchitektur heute kaum ein Weg vorbeiführt, zeigt die bisherige Argumentation nur die halbe Wahrheit, denn das reale Szenario ist wesentlich komplexer. So würde eine IT-Security, die sich ausschließlich auf den Schutz der Cloud konzentriert, eine Infektion der lokalen Arbeitsplätze (Clients bzw. Endpoints) in Kauf nehmen, was zunächst akzeptabel erscheint. Denn: Moderne Cloud-Systeme reduzieren die Rolle der Endpoints dank SaaS, IaaS, MaaS und PaaS auf die eines einfachen Benutzer-Interfaces. Hinzu kommt die Tatsache, dass die Clients für Angreifer praktisch uninteressant sind, wenn an dieser Stelle keine nutzbaren Daten vorhanden sind. Doch das stimmt nicht ganz, denn ein Endpoint ist im Moment der Datenübertragung hochverletzlich und wird spätestens dann zur potenziellen Schwachstelle. Daher müssen Anwender, die auf eine professionelle Cloud Security setzen, auch ihre Endpoints bzw. Clients sichern. Hierfür bieten die meisten Cloud-Spezialisten entsprechende Endpunkt-Sicherheitslösungen mit erweiterten clientseitigen Security Tools an, die in der Regel per-

fekt auf die jeweiligen Cloud-Technologien abgestimmt sind, zentral verwaltet werden und den Anwendern vor Ort kein erweitertes Know-how abfordern. Hierzu gehören beispielsweise folgende Werkzeuge bzw. Maßnahmen:

- Das Betriebssystem immer auf dem aktuellen Stand halten
- Spezieller Browser-Schutz mit Firewalls und Intrusion Detection sowie Antiviren- und Internet-Security-Tools für mobile Geräte
- Multi-Factor-Authentifizierung (MFA) mit besonders starken Passwort-sicherheitsrichtlinien zur Prävention unbefugter Zugriffe
- Software mit bekannten Sicherheitslücken entfernen – besser gar nicht erst einsetzen
- Spezielle Backup- und Recovery-Tools zur Sicherung der lokalen Daten auf externen Speichermedien

Um großen, komplexen Angriffen einen effizienten Schutz entgegenzusetzen, schädlichen Traffic zu erkennen und von Anfang an robuste Abwehrmaßnahmen nutzen zu können, werden die entscheidenden Maßnahmen innerhalb der Cloud realisiert, wobei ein effizientes Backup und eine gezielte Früherkennung von zentraler Bedeutung sind. Dies bestätigen die Experten von Gartner in ihrem Bericht zum Thema Ransomware Backup vom Januar 2021. Gartner stellt darin fest, dass die von den meisten Organisationen eingesetzte Anti-Malware- und Antiviren-Software nicht genügt, um echte Ransomware-Resilienz zu erreichen. Im Gegensatz dazu kann die cloudbasierte IT-Security allein durch die hohe Kapazität und Performance des Backend-Systems deutlich mehr Sicherheit gewährleisten und etwa im DDoS-Bereich entscheidend dazu beitragen, dass schädlicher Traffic eine Website gar nicht erst erreicht oder dass die Kommunikation über eine Web API beeinträchtigt wird. In diesem Zusammenhang steht den Cloud-Anbietern eine Vielzahl von hocheffizienten Werkzeugen zur Verfügung, die den dynamisch veränderlichen Angriffsvektoren moderner DDoS- und Ransomware-Attacken gewachsen sind und die Anwender somit zuverlässig schützen können. Daher sollten Cloud-Kunden darauf achten, dass ihr Cloud-Security-Paket neben SaaS-, IaaS- und MaaS-Funktionen auch beispielsweise folgende Dienstleistungen beinhaltet:

- Anomalie-Erkennung
- Schwachstellen-Scans
- Identifizierung kritischer IP-Adressen
- Schließen bekannter Sicherheitslücken
- Filterung von schädlichem Traffic
- DDoS Cloud Scrubbing
- Integration der oben genannten Endpoint Security Tools
- Sicherer, redundanter und vom Netzwerk getrenntes Enterprise Level Backup

4.3 Backup

Eine gute Backup-Strategie ist eine wesentliche Maßnahme gegen einen kriminellen Angriff auf ein Unternehmensnetzwerk – auch und vor allem in der Cloud. Richtig umgesetzt kann sie selbst die Schäden einer hochkomplexen DDoS- oder Ransomware-Attacke ins Leere laufen lassen oder auf ein Minimum reduzieren und Unternehmen bzw. Einrichtungen in kürzester Zeit wieder vollständig arbeitsfähig machen. Im Zeitalter der globalen Vernetzung macht es gerade im professionellen Umfeld kaum noch Sinn, den Schutz für jedes einzelne Gerät dezentral zu installieren. Einerseits wäre das viel zu aufwändig und auf der anderen Seite würde sich die Zahl der Angriffspunkte so um ein Vielfaches erhöhen. Da DDoS- und Ransomware-Angriffe naturgemäß in vernetzten Systemen stattfinden, scheint es vor allem im Bereich des Backups logisch, das Angriffspotenzial auf einen einzigen Bereich zu reduzieren, der mit professionellem Know-how und optimierten Technologien geschützt werden kann.

Diese Chance haben viele Unternehmen und Einrichtungen bereits erkannt und damit begonnen, ihre IT-Security inklusive Backup an professionelle Dienstleister auszulagern. Diese setzen mittlerweile auf zukunftsfähige SaaS-, IaaS-, MaaS- und PaaS-Dienstleistungen, bei denen alle wichtigen Daten ohnehin zentral verarbeitet werden. Bei den Anwendern vor Ort verbleiben wie zuvor beschrieben somit nur noch ganz einfache Clients, die als vernetzte Anzeigegeräte ohne größeren Software- und Datenbestand auskommen.

Aber zurück zu den Anforderungen an das professionelle Backup in der Cloud. Für dieses haben die Spezialisten von Gartner eine Reihe von kritischen Funktionen definiert, die ein professionelles Cloud-Paket enthalten sollte. Aus Sicht von Gartner gehören Folgende zu den Wichtigsten:

Skalierbarkeit	Die Speicher- und Rechenkapazität des Backup-Systems und die E/A-Bandbreite sollten in der Lage sein, mit der Speichermenge des Anwenders zu wachsen.
Effizienz	Das Backup-System sollte in Bezug auf Speicherauslastung, Bandbreitenverbrauch und Ressourcen effizient arbeiten.
Leistung	Das Backup-System sollte ausreichend Performance bieten, um Backup- und Recovery-Vorgänge zeitnah zu realisieren.
Fügsamkeit und Benutzerfreundlichkeit	Das Backup-System sollte die Arbeit des Sicherungsadministrators vereinfachen – z.B. bei der Erstellung von Sicherungsaufträgen oder der selektiven Wiederherstellung einzelner Dateien bzw. E-Mails oder Datenbankdatensätze. Wichtige Funktionen sollten dabei automatisiert erfolgen.
Unterstützung für verschiedene Arten von Daten	Das Backup-System sollte in der Lage sein, sowohl strukturierte als auch unstrukturierte Daten zu schützen und effizient auf großen Network-Attachaed-Storage (NAS)-Plattformen zentral zu sichern. Hierzu gehören auch Daten aus SaaS-Anwendungen.
Sicherheit	Das Backup-System sollte wichtige Sicherheitsfunktionen wie die Fähigkeit zur Verschlüsselung während der Sicherungsvorgänge und die Unterstützung einer rollenbasierten Zugriffskontrolle (RBAC) etc. beinhalten.
Ransomware-Schutz	Das Backup-System sollte die Sicherungsdaten vor Ransomware-Angriffen schützen und eine schnelle Wiederherstellung von Daten nach einem möglichen Angriff ermöglichen. Zusätzlich zu diesen von Gartner definierten Kriterien sollte das Backup-System aber auch einen Schutz gegen DDoS-Attacken bieten.
Berichte und Analysen	Das Backup-System sollte Anwender mit regelmäßigen, gut nachvollziehbaren Berichten über wichtige Aspekte informieren. Diese sollten z. B. den Speicherverbrauch, die Erfolgsrate von Sicherungsaufträgen und die Analyse der Sicherheit des Sicherungssystems beinhalten.

Somit ergeben sich hohe Anforderungen an Cloud-Dienstleister, beim Thema Backup für den Kunden mitzudenken. Durch ein externes Backup schaffen sie nicht nur eine zusätzliche Schnittstelle, die gegen Angriffe geschützt werden muss. Vielmehr entsteht vor allem bei einem Backup außerhalb der EU eine zusätzliche Gefahr, die vielen Kunden nicht bewusst ist: US-Unternehmen sind per Gesetz (US CLOUD Act) spätestens seit 2018 verpflichtet, die Daten ihrer Kunden bei Bedarf an die Behörden ihres Landes weiter zu leiten. Damit verlieren sie jede Kontrolle über diese Daten und ihre Kunden wissen nicht,

was mit den Daten geschieht. Ein angemessenes Schutzniveau für persönliche Daten besteht in den USA nach Ansicht des Europäischen Gerichtshofs (EuGH) nicht – auch nicht bei datenspeichernden und verarbeitenden Providern mit Muttergesellschaft in den USA.

Aufgrund dieser Situation sollten die Cloud-Anbieter ihren Kunden in jedem Fall unmissverständlich mitteilen, ob sie Daten extern speichern und welche Schutzmaßnahmen sie in Bezug auf den US CLOUD Act anbieten. Denn nur so können sie eine ausreichend hohe Datensouveränität garantieren, die vor allem für Anwender im Bereich der öffentlichen Hand von elementarer Bedeutung ist.

Die grundlegende Aufgabe des Backups ist die Möglichkeit, Daten bei Verlust oder ungewollter Veränderung – etwa durch einen Hacker-Angriff – wieder herzustellen. Dafür werden die Daten sicher gespeichert und vor fremdem Zugriff geschützt. Dabei spielen die Verschlüsselung der Daten sowie eine vom Internet getrennte Speicherung eine wesentliche Rolle. Ist das garantiert, lassen sich die Daten kaum noch für eine gezielte Erpressung im Rahmen eines Ransomware-Angriffs nutzen. Hierfür haben die Experten von Gartner nützliche Regeln aufgestellt und in ihrem Ransomware Backup Report veröffentlicht. Hierzu gehören beispielsweise:

Mithilfe eines Backups lassen sich Daten bei Verlust oder ungewollter Veränderung wieder herstellen.

- Das Vermeiden oder Beseitigen von Netzwerkfreigabe-Protokollen wie CIFS oder NFS
- Die Backup-Administrationskonsole sowie die Kopien der Backup-Daten sind zuverlässig zu schützen
- Um unautorisierte Zugriffe zu verhindern, sind administrative Konten durch Multifaktor-Authentifizierung zu sichern
- Die Ransomware-Wiederherstellung sollte in einer isolierten Umgebung stattfinden, um weitere Infektionen auszuschließen

Ungeachtet dieser Maßnahmen müssen Anwender immer davon ausgehen, dass ihre Backups potenziell infiziert sind, denn Malware könnte schon vor dem Erstellen des Backups unbemerkt eingedrungen sein. In den verschiedensten Dateien kann sie für lange Zeit unsichtbar auf ihre Aktivierung warten. Hier kann selbst ein Malware-Scan beim Erstellen des Backups keine hundertprozentige Sicherheit garantieren, auch wenn dieser dringend empfohlen wird. Mittlerweile werden hierbei auch neuartige, etwa KI-basierte Technologien angeboten, die das Risiko der Malware-Infektion weiter senken können. Es bleibt stets ein Restrisiko, das sich durch den Einsatz von redundanten Mehrfach-Backups reduzieren, aber niemals komplett ausschalten lässt. Dennoch gibt es auch weiterführende Methoden, die dazu beitragen, das Infektionsrisiko zu senken. Hierzu gehören unveränderliche Dateispeicher, die eine bestimmte Aufbewahrungsfrist garantieren. Mit diesen ist es nahezu ausgeschlossen, dass ein Datensatz für eine bestimmte Dauer gelöscht, modifiziert oder überschrieben wird. Kommt es zwischenzeitlich zu einem Angriff, stehen die Daten weiterhin zur Verfügung.

4.4 Recovery

Eine weitere kritische Aufgabe ist der Wiederherstellungsprozess (Recovery). Auch hierbei können Fehler auftreten oder Viren eindringen – vor allem wenn es darum geht, riesige Datenmengen von Hunderten oder gar Tausenden Servern wieder herzustellen. Daher sollte dieser Prozess systematisch erfolgen – Experten sprechen dabei auch von einer sogenannten ‚Orchestrierung'. Hierbei geht es vor allem um eine klar definierte Wiederherstellungsreihenfolge, denn nicht alle Applikationen dürfen gleichzeitig starten und in vielen Fällen gibt es sogenannte Recovery Time Objectives (RTO). Das Ziel dieses Prozesses ist es, besonders wichtige Applikationen schnell wieder online zu schalten, wobei sichergestellt sein muss, dass Anwendungen, die für deren Sicherheit zuständig sind, zuvor gestartet worden sind. Zudem sollte die jeweils mit der Anwendung verbundene und wiederherzustellende Datenmenge mit in die Kalkulation eingerechnet werden.

Aber auch die einzelnen Daten sollten klar priorisiert werden. Anwender müssen vorab definieren, welche Daten bei einem möglichen Angriff unbedingt erhalten bleiben müssen und welche eventuell auch verloren gehen dürfen. Diese sogenannte Recovery Point Objective (RPO)-Strategie ist darauf ausgerichtet, dass der Verlust von Daten aus den letzten Stunden gezielt in Kauf genommen wird, während überlebenswichtige Stammdaten mehrfach gespeichert und gegen Veränderung geschützt werden, damit sie im Notfall jederzeit sicher wiederhergestellt werden können. In diesem Zusammenhang stellt sich die Frage nach realistischen Sicherungsintervallen, um so zu definieren, wie lange ein System maximal ausfallen darf, ohne dass entscheidende Daten endgültig verloren gehen. Auch hier spielt das Thema RTO eine wichtige Rolle.

Um alle Voraussetzungen für den Ernstfall zu schaffen, sollten Anwender zudem einen sogenannten Disaster-Recovery-Plan vorbereiten, der bei Bedarf aktiviert werden kann. Dieser beinhaltet eine ausführliche Dokumentation, die minutiös festlegt, wie bei einem schwerwiegenden Ausfall zu verfahren ist und wer dabei welche Aufgaben innehat. Hierbei sollten Punkte wie der generelle Aufbau der Infrastruktur – egal ob diese On-Premises oder in der Cloud realisiert wird – feingranular dokumentiert sein. Hinzu kommt eine schrittweise Anleitung zur Wiederherstellung von Services inklusive aller notwendigen Konfigurationen wie IP-Adressen, DNS-Konfigurationen, Firewalls, Routing.

Für den Ernstfall sollten Anwender einen Disaster-Recovery-Plan vorbereiten, der minutiös festlegt, wie bei einem schwerwiegenden Ausfall zu verfahren ist.

5 Souveräne Digitalisierung in Sicherheit – so kann sie gelingen

5.1 Datensouveränität ist nicht nur eine Frage des Rechts

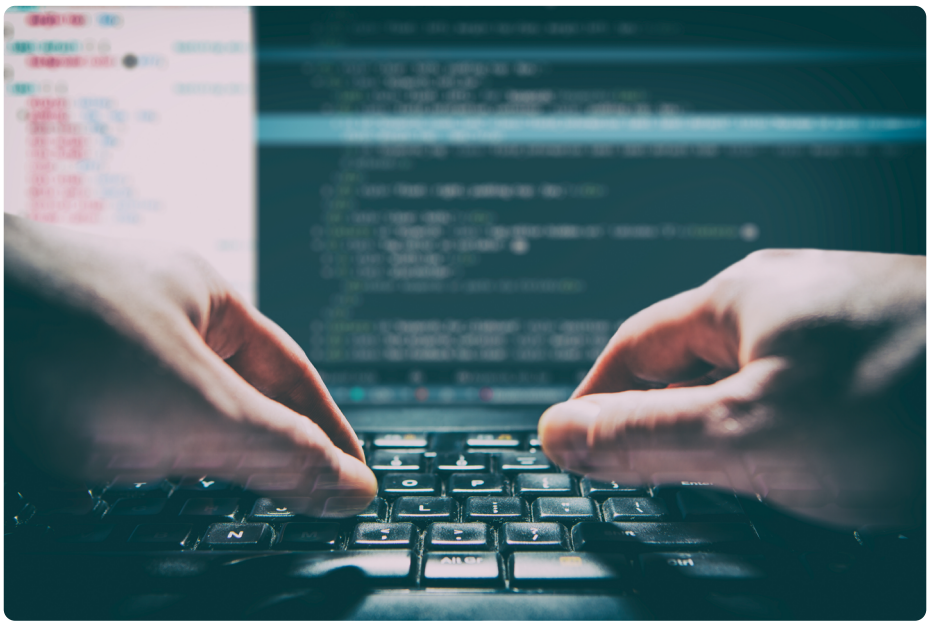
Der Bereich der IT-Security ist riesig und der Markt wächst rasant. Mittlerweile bieten zahlreiche Anbieter cloudbasierte Lösungen an, die einen zuverlässigen Schutz gegen Ransomware- und DDoS-Attacken beinhalten – auch für mittlere und größere Unternehmen sowie Einrichtungen der öffentlichen Hand. Beispiele dafür sind Akamai, Bechtle, Bitdefender, Cloudflare, Dynatrace, F5 Networks, Fastly, IONOS, Juniper, Palo Alto Networks, Zscaler und viele andere. Ein Großteil dieser Anbieter ist in den USA beheimatet und unterliegt daher dem zuvor genannten US CLOUD Act, der die Übertragung von gespeicherten Daten in die USA nicht nur ermöglicht, sondern ausdrücklich einfordert – selbst dann, wenn die Speicherung nicht in den USA erfolgt. Um dem zu entgehen, können Anwender auf europäische Anbieter setzen, denen die Sicherheit ihrer Kundendaten ein zentrales Anliegen ist. Um Anwendern Orientierung zu bieten und die Auswahl des jeweils geeigneten Dienstleisters zu unterstützen, hat das BSI spezielle Richtlinien veröffentlicht, die vom jeweiligen Cloud-Anbieter verbindlich zugesichert werden müssen, um eine tatsächliche Souveränität der Daten zu gewährleisten. Hierzu gehören folgende:

- Keine Abhängigkeit von ausländischen Interessen
- Keine Übermittlung von Daten an Drittländer
- Datenverarbeitung in Deutschland
- Transparente System- und Leistungsbeschreibung
- Zertifizierung durch unabhängige Dritte
- Unterstützung für mindestens einen offenen Standard im Sinne von , Infrastructure as Code‘

Darüber hinaus bietet die europäische Initiative Gaia-X interessante Anknüpfungspunkte. Im Rahmen dieser Initiative arbeiten Unternehmen und Experten aus Wirtschaft, Wissenschaft und Politik an der Gestaltung eines vitalen, offenen und transparenten digitalen Ökosystems, das den höchsten Ansprüchen an die digitale Souveränität auf europäischer Ebene gerecht werden kann und Innovationen gezielt fördert. Damit sollen letztendlich Daten und Dienste verfügbar gemacht, zusammengeführt, vertrauensvoll geteilt und genutzt werden können. Hierfür setzen die Vertreter von Gaia-X auf Open-Source-Lösungen als zentrales Fundament für die digitale Souveränität der Anwender. Open Source steht für technische Unabhängigkeit und ermöglicht eine selbstbestimmte Entwicklung, ohne dass die Anwender in die Abhängigkeit von einzelnen Anbietern (sogenannter ‚Vendor-Lock-Ins‘) geraten. Dieser würde sie langfristig an bestimmte Technologien oder Standards binden. Zudem lassen sich Open-Source-Systeme individuell anpassen und arbeiten mit einer Vielzahl von Schnittstellen oder sogar mit offenen, programmierbaren Interfaces (APIs).

5.2 Worauf ist bei der Wahl der richtigen Lösung und des richtigen Partners zu achten?

Selbst für große Unternehmen, die heute oftmals auf eigene In-House-Lösungen oder hybride Architekturen setzen, ist eine cloudbasierte IT-Security interessant, denn mit der ‚Auslagerung' dieser anspruchsvollen Aufgabe können sie sich wieder mehr auf ihre Kernkompetenzen konzentrieren. Die Cloud-Anbieter verfügen über das richtige Know-how, um bei Bedarf auch individuelle Cloud-Lösungen zu installieren, die den Anwender in dieser wichtigen Aufgabe entlasten und dennoch alle lokalen Niederlassungen in eine sichere Netzwerkinfrastruktur einbinden können. Grundsätzlich sollten Anwender bei der Wahl des Cloud-Partners einen Blick auf das Thema Datensouveränität werfen, damit sie sicherstellen, dass keine Daten in die Hände von Dritten gelangen können.



6 DDoS in der Praxis

In diesem White Paper wurden bereits viele Angriffsszenarien und zahlreiche Schutzmaßnahmen beschrieben. Doch wie sieht das in der Praxis aus? Was geschieht im Hintergrund, wenn sich ein Unternehmen oder eine Einrichtung für die Zusammenarbeit mit einem professionellen Cloud Security Provider entscheidet?

In der Regel wird dieser Schutz innerhalb der Cloud unsichtbar realisiert und selbst bei einem Angriff werden Anwender nur über eine erfolgreiche Abwehr informiert. Doch die tatsächlichen Aufgaben der Security-Experten sind hochanspruchsvoll und aufwändig. Fast immer sorgt ein großes Team an gut ausgebildeten Netzwerkspezialisten rund um die Uhr dafür, dass Schutzmechanismen nicht entschlüsselt, unterlaufen oder missbraucht werden. Dafür müssen komplexe Prozesse lückenlos Hand in Hand greifen. Kein Wunder, dass die Cloud-Security-Zentren wie Festungen ausgebaut werden, aus denen kaum etwas nach außen dringt.

Diese Strategie verfolgen praktisch alle großen Cloud Security Provider und auch bei IONOS ist das nicht anders. Der Netzwerkspezialist aus dem Rheinland-Pfälzischen Montabaur arbeitet mit einem eigenen Backbone und betreibt acht weltweit verteilte Scrubbing Center sowie eine selbst entwickelte DDoS-Defense-Plattform. Über dieses engmaschige System fließt der gesamte Datenverkehr der IONOS Kunden, wodurch diese einen großen Vorteil erhalten: IONOS überwacht den Daten-Traffic seiner Kunden lückenlos selbst und kann im laufenden Betrieb früh auf Anomalien und verdächtige Inhalte zugreifen, um sie genauer zu analysieren, zu blockieren oder zu desinfizieren. Werden diese Daten nach Analyse und Reinigung im Scrubbing Center (wieder) als ‚sauber' klassifiziert, leitet sie das System umgehend an das jeweils zuständige Data Center und somit an den entsprechenden Kunden weiter. Diese merken die damit verbundene Verzögerung kaum, denn diese ist minimal und steht in keinem Verhältnis zu den oft wochenlangen Ausfällen, die eine DDoS- oder eine Ransomware-Attacke verursachen kann.

IONOS arbeitet mit einem eigenen Backbone und betreibt weltweit acht Scrubbing Center und eine selbst entwickelte DDoS-Defense-Plattform.

Ebenso spricht das enorme technische Potenzial für den Einsatz eines Cloud-Security-Systems, das in einer lokalen Sicherheitsarchitektur kaum zur Verfügung steht. So besitzt IONOS über genügend eigene Ressourcen, um DDoS-Attacken mit einem Volumen von bis zu 1 Tbit/Sekunde erfolgreich abzuwehren. Dieses Potenzial liegt weit über dem üblichen Traffic eines großen DDoS-Angriffs, der fast immer deutlich unter 100 Gbit/Sekunde bleibt. Hinzu kommt eine Vielzahl von bewährten Schutzmaßnahmen, die das Unternehmen über Jahre hinweg installiert, selbst entwickelt und aufgrund der eigenen Erfahrungen mit erfolgten Angriffsversuchen immer weiter optimiert hat.

Weitere Informationen hierzu finden Sie in diesem Videobeitrag.

7 DoS- und Ransomware-Schutz der Zukunft

In der Studie zur Lage der IT-Sicherheit in Deutschland 2021 stellt das BSI eindeutig fest, dass es trotz aller Prävention auch in Zukunft nicht möglich sein wird, sich vollständig gegen Angriffe zu schützen. Doch mit den richtigen Werkzeugen und professionellem Management lassen sich die Risiken zweifelsohne deutlich reduzieren. Daher sollten Unternehmen und Einrichtungen, die mit sensiblen Daten oder vernetzten Systemen arbeiten, über eine cloudbasierte Security nachdenken. So können sie sich auf ihre eigentliche Arbeit konzentrieren, während sie das anspruchsvolle IT-Sicherheitsmanagement entspannt in professionelle Hände legen. Dennoch lohnt sich an dieser Stelle auch ein Blick in die Zukunft, denn die Bedrohungslage ist hochdynamisch und kriminelle Angreifer entwickeln ständig neue Methoden. Angesichts der Tatsache, dass Ransomware mittlerweile als kriminelle Dienstleistung (RaaS, s.o.) aus der Cloud angeboten wird, sollten IT-Verantwortliche aller Branchen neue Angriffsmethoden und Technologien im Auge behalten. Bereits jetzt zeichnen sich verschiedene Entwicklungen in Zusammenhang mit beispielsweise Künstlicher Intelligenz, Kryptowährungen, DeepFakes und Schatten-IT ab (vgl. u.a. Sophos Thread Report 2022 und ESET Security Trends 2022).

Neben diesen ohnehin massiven Bedrohungen sieht ESET Security vor allem auch die Gefahr einer Zunahme von Angriffen auf kleine und mittlere Unternehmen sowie auf Städte und Gemeinden, nachdem das Unternehmen schon im Jahr 2021 eine deutliche Verschärfung der Angriffsszenarien auf kommunaler Ebene verzeichnen konnte.[7] Gerade hier sind die Möglichkeiten für den Schutz der eigenen IT-Systeme und Netzwerke oftmals nicht ausgereizt.

Angesichts dieser Entwicklungen wird die Überwachung durch einfache Sicherheits-Tools zukünftig nicht mehr ausreichend sein. Stattdessen sollten Unternehmen und Einrichtungen auf eine gezielte Kombination von hochleistungsfähigen Erkennungsmethoden setzen und diese stets auf dem aktuellsten Stand halten. Hierbei kann eine cloudbasierte Security, die den Traffic als zentrale Festung professionell überwacht und analysiert, im entscheidenden Moment die erforderliche Sicherheit bieten.

7. B2B Cyber Security (2022): ESET SECURITY TRENDS 2022: RANSOMWARE, DDOS & CO, online verfügbar unter: https://b2b-cyber-security.de/en/eset-security-trends-2022-ransomware-ddos-co/.

IONOS

Über IONOS

IONOS ist mit mehr als acht Millionen Kundenverträgen der führende europäische Anbieter von Cloud-Infrastruktur, Cloud-Services und Hosting-Dienstleistungen. Das Produktportfolio bietet alles, was Unternehmen benötigen, um in der Cloud erfolgreich zu sein: von Domains über klassische Websites und Do-It-Yourself-Lösungen, Online-Marketing-Tools bis hin zu vollwertigen Servern und einer IaaS-Lösung. Das Angebot richtet sich an Freiberufler, Gewerbetreibende und Konsumenten sowie an Unternehmenskunden mit komplexen IT-Anforderungen.

IONOS Cloud ist die europäische Cloud-Alternative und Teil von IONOS. Unser Produktportfolio umfasst mit der Cloud Compute Engine eine IaaS Compute Engine mit eigenem Code Stack für Virtualisierung, Managed Kubernetes für Container-Anwendungen, eine Private Cloud powered by VMware sowie S3 Object Storage. Mit unserem Angebot bieten wir etablierten mittelständischen und großen Unternehmen, regulierten Industrien, der Digitalwirtschaft und dem öffentlichen Sektor alle notwendigen Dienste und Services um in und mit der Cloud erfolgreich zu sein.

IONOS entstand 2018 aus dem Zusammenschluss von 1&1 Internet und dem Berliner IaaS-Anbieter ProfitBricks. IONOS ist Teil der börsennotierten United Internet AG (ISIN DE0005089031). Zur IONOS Markenfamilie gehören STRATO, Arsys, Fasthosts, home.pl, InterNetX, SEDO, United Domains und World4You.

Mehr Informationen verfügbar unter https://cloud.ionos.de/

Impressum

IONOS SE
Berlin Office
Revaler Straße 30
10245 Berlin, Germany

IONOS Cloud Kontakt

Telefon +49 30 57700 840
Telefax +49 30 57700 8598
E-Mail produkt@cloud.ionos.de
Website https://cloud.ionos.de

Vorstand

Hüseyin Dogan, Dr. Martin Endreß, Claudia Frese, Hans-Henning Kettler, Arthur Mai, Britta Schmitt, Achim Weiß

Aufsichtsratsvorsitzender

Markus Kadelke

Handelsregister

IONOS SE: Amtsgericht Montabaur / HRB 24498

Umsatzsteuer-IdentNummer

IONOS SE: DE815563912

Copyright