



Wie sicher ist die Cloud wirklich?

RISIKEN RICHTIG EINSCHÄTZEN UND VORKEHRUNGEN TREFFEN

www.link11.com

Wie sicher ist die Cloud wirklich? Risiken richtig einschätzen und Vorkehrungen treffen

Die Nutzung der Cloud gehört inzwischen weltweit in vielen Unternehmen zum Alltag. Sie erleichtert die Vernetzung von Standorten und Systemen, schafft mehr Flexibilität und reduziert Kosten. Die eigentlich segensreiche Erfindung kann sich aber rasch zu einem Fluch entwickeln, der Unternehmen bis ins Mark erschüttert, wenn das Thema Sicherheit unterschätzt wird.

Die Nutzung von Cloud-Diensten hat sich in Unternehmen etabliert. Nach Informationen des „Cloud Monitors 2019“ des Branchenverbandes Bitkom und des Beratungsunternehmens KPMG setzen inzwischen drei von vier Unternehmen auf das Cloud-Computing.¹ International sind es laut „RightScale 2019 State of the Cloud Report“ von Flexera sogar 94 Prozent. Es gibt viele Argumente, die zugunsten der Cloud sprechen.²

Aber die wachsende Abhängigkeit von Cloud-Anwendungen bringt auf der anderen Seite enorme Risiken mit sich. Eine Cyberattacke auf eine geschäftskritische Anwendung führt im schlimmsten Fall bis zum Stillstand der gesamten Organisation.

Die Abhängigkeit von der Cloud ist auch gefährlich

Es liegt in der Natur der Sache, dass die Anbindung an das öffentliche Netz ein Einfallstor für Angreifer mit Überlastungsangriffen ist. Die Vorteile, die die Cloud den Unternehmen bietet, haben Cyberkriminelle längst für sich entdeckt. Sie mieten ebenfalls unkompliziert Rechenkapazitäten von Public-Cloud-Anbietern an und nutzen diese für ihre Zwecke.

Besondere Gefahr droht aus Überlastungsangriffen (DDoS), die die Anbindung an die Cloud oder darüber verbundene Systeme zum Ziel haben. Der Zusammenbruch des Internetzugangs oder die Schwächung der Systeme hat dann empfindliche und teure Folgen:

- Der Betrieb wird unterbrochen. Der Zugriff auf wichtige Systeme ist nicht möglich. Hängt beispielsweise die Telefonanlage an der Cloud, ist das Unternehmen nicht zu erreichen.
- Anwendungen in der Cloud werden teilweise zur Produktionssteuerung genutzt. Eine Unterbrechung des geregelten Ablaufs äußert sich in Unterbrechungen oder nicht einzuhaltende Termine oder Liefermengen.
- Die Produktivität im Unternehmen wird empfindlich gestört, weil Mitarbeiter im Innen- und Außendienst nicht auf Anwendungen oder Daten zugreifen können.

Die aus den Störungen erwachsenen Folgen für das Unternehmen sind stets die gleichen. Es kommt zu Verlusten des Ansehens bei Kunden, Lieferanten und Geschäftspartnern. Mittelbar und unmittelbar kosten die Ausfälle bares Geld, etwa durch entgangene Umsätze.

Welche Dimensionen solche Ausfälle der Cloud inzwischen annehmen können, hat sich im Oktober 2019 eindrucksvoll gezeigt. Seinerzeit kam es durch DDoS-Attacken in Teilen zu Ausfällen bei Amazons S3-Angebot (Simple Storage Service).³ Über Stunden konnten viele Unternehmen, die diese Infrastruktur nutzen, nicht auf ihre Instanzen zugreifen. Der Schaden bei den Anwenderunternehmen dürfte sich auf über 100 Millionen US-Dollar summieren.

Besonders spektakuläre Angriffsversuche gegenüber Unternehmen und Regierungseinrichtungen basierten in der Vergangenheit oft auf Botnetzen, die Komponenten des IoT zusammenschlossen. Im Rahmen des DDoS-Halbjahresreports des LSOC (Link11 Security Operation Center) für die erste Jahreshälfte 2019 offenbarte sich, dass bei mindestens jedem dritten Überlastungsangriff (38 Prozent) bereits Cloud-Server beteiligt waren. Zum Vergleich: Im ersten Halbjahr 2018 lag dieser Anteil noch bei 26 Prozent.⁴

Es sind nüchterne Überlegungen, die Angreifer zu diesem Wechsel ihres Vorgehens bewogen haben. Denn während Router oder Überwachungskameras meist mit nur wenigen Mbps angebunden sind, bieten die Cloud-Instanzen deutlich größere

Bandbreiten zwischen 1 und 10 Gbps. Ihr Angriffsvolumen kann daher bis zu 1.000x höher als bei einzelnen IoT-Geräten sein.

In vielen Unternehmen halten Sicherheitskonzepte nicht mit diesen aktuellen Entwicklungen Schritt. Häufig verlassen sich CIO, CDO und Administratoren auf die klassischen Firewall-Systeme am strategisch wichtigen Übergabepunkt zwischen internen Strukturen und Internet oder setzen auf Konzepte wie demilitarisierte Zonen.

Herkömmliche Sicherheitskonzepte bieten keinen ausreichenden Schutz

Die einfachste Möglichkeit für Unternehmen, sich gegen die besonders gefürchteten DDoS-Attacks zu wehren, scheint das Blockieren von Cloud-Services zu sein, sofern die Angriffe aus Amazon oder Azure heraus erfolgen. Da die Firmen vielfach auf diese Dienste selbst zugreifen, wäre somit auch die eigene Anbindung unterbrochen und Geschäftsprozesse kämen zum Stillstand.

Mit einer Web-Application-Firewall (WAF) kann legitimer Cloud-Traffic auf eine Whitelist gesetzt werden. Um ihren Nutzen zu entfalten, müsste der Datenverkehr möglichst frühzeitig analysiert werden. Die Firewall liegt jedoch hinter dem Wide-Area-Anschluss (WAN). Der kann durch die Attacke blockiert sein, bevor überhaupt eine Filterung stattgefunden hat.

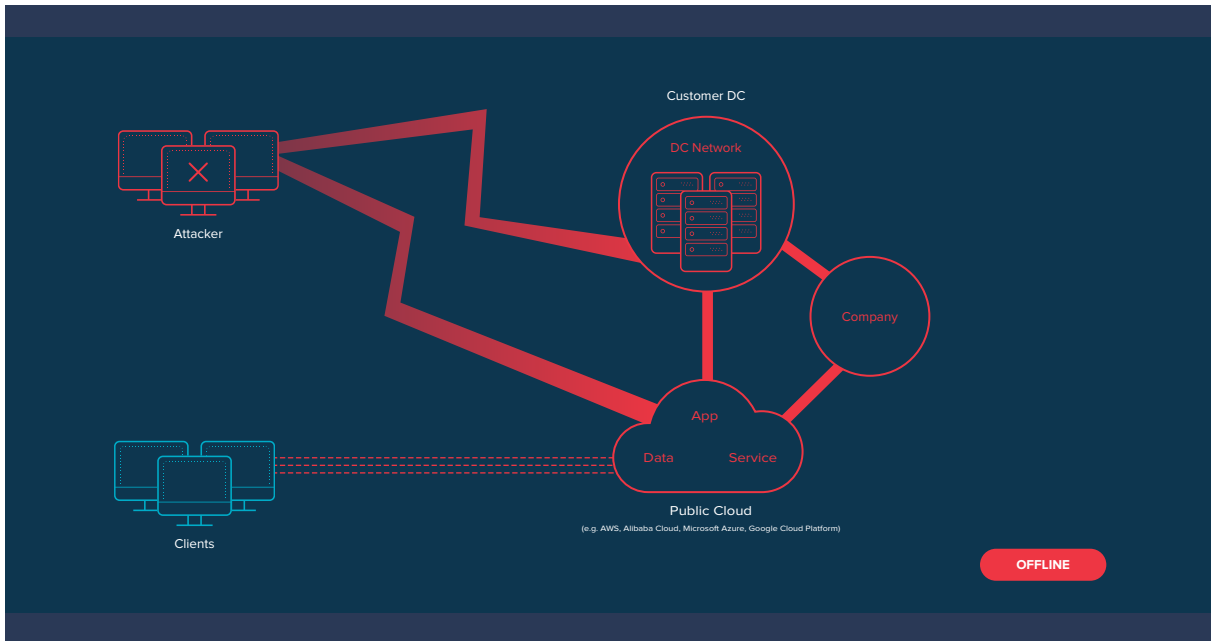
Völlig wirkungslos bleiben alle im Rechenzentrum getroffenen Maßnahmen, wenn die Instanz eines in der Cloud laufenden Systems aus derselben Umgebung angegriffen wird. Denn die Anfragen gelangen gar nicht erst zur eigenen Firewall. Der per virtueller Maschine bei Azure oder Amazon gehostete Shop oder das CRM gehen so offline oder werden so beeinträchtigt, dass ein vernünftiges Arbeiten nicht mehr möglich ist.

Setzen Firmen zusätzlich zur Web-Application-Firewall auf Maßnahmen vor DDoS-Attacks durch dedizierte eigene Hardware-Appliances arbeiten deren Filtermechanismen nur so lange, wie die externe Anbindung nicht überlastet wird. Die meisten Unternehmen nutzen Anschlüsse im Bereich von 1 bis 10 Gbps. Link11 stellt in der Vergangenheit aber immer häufiger Attacks im dreistelligen Gbps-Bereich fest. Gegenüber solchen brandbreitenstarken Angriffen direkt aus der Cloud sind Appliances unterlegen.

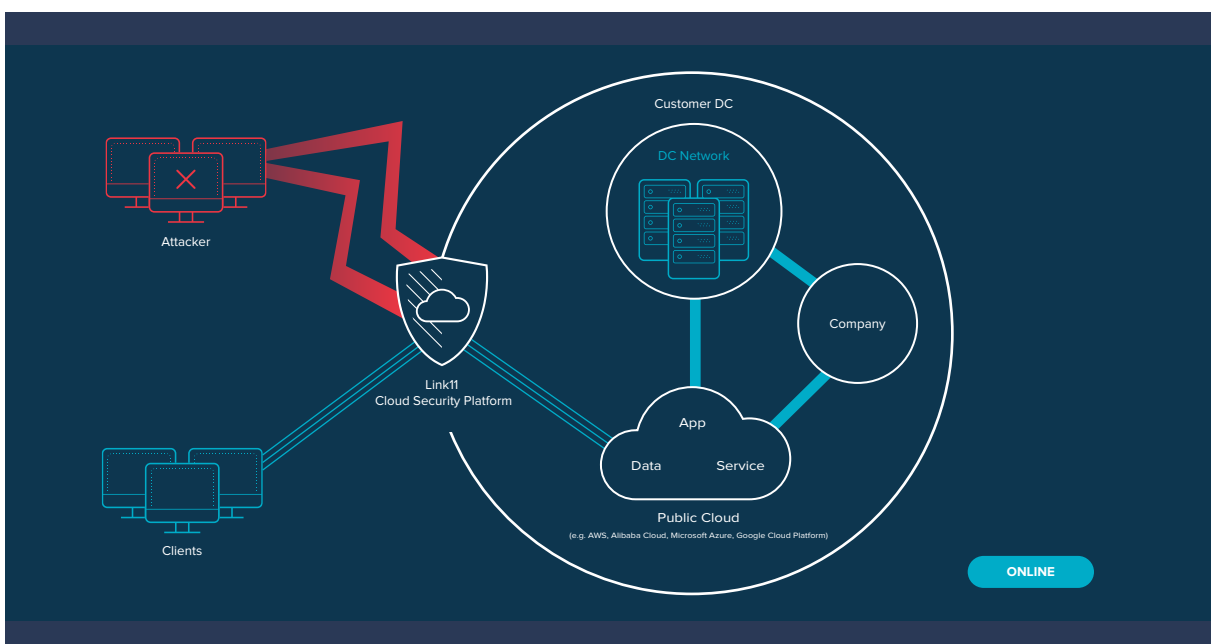
Große Organisation, die sehr viel Datenverkehr über die Cloud abwickeln, können mit dem Cloud-Anbieter Direktverbindungen aufbauen. Eine solche dedizierte private Cloud-Anbindung (Private Peering) ist aber nur für sehr wenige Unternehmen überhaupt finanziell darstellbar. Doch selbst diese Anbindung hat ohne den Einsatz weiterer Sicherheitsmechanismen Schwächen. Ein Angriff aus der gleichen Cloud-Umgebung kann die Anbindung mit illegitimen Datenpaketen verstopfen.

Schutz vor DDoS-Attacken auf Unternehmen mit virtuellen und lokalen IT-Systemen

Der Trend geht von der privaten Cloud hin zur Public-Cloud, bei der Daten, Services und Applikationen extern auf den Servern der Cloud-Anbieter aufbewahrt werden. Diese sind mit der lokalen IT des Unternehmens vernetzt. Erfolgreiche DDoS-Angriffe auf nur einen Teil dieser Infrastruktur können daher auch alle anderen Systeme und Plattformen schädigen.



Eine kontinuierliche Überwachung der gesamten virtuellen und lokalen IT-Infrastruktur sowie die Filterung des Datenverkehrs sind der beste Schutz gegen DDoS-bedingte Ausfälle. Dafür wird der Datenverkehr durch einen externen Filtercluster geleitet. Im Scrubbing Center wird der Angreifer-Traffic von legitimen Client-Zugriffen getrennt.



So wenden moderne Sicherheitskonzepte von Link11 die Gefahren ab

Die wachsende Komplexität von Angriffsszenarien führt einfache regelbasierte Systeme, die mit Whitelists arbeiten, an ihre Grenzen. Zeitgemäßen Schutz bieten Lösungen, die zusätzlich künstliche Intelligenz nutzen. Durch maschinelles Lernen während der dauerhaften Analyse des Datenverkehrs wird Wissen über das Kommunikationsprofil des erlaubten Datenverkehrs aufgebaut. Abweichungen von diesem Normalzustand werden zuverlässig und schnell erkannt. Die Technologie ermöglicht auch Eingriffe mit einer höheren Granularität. Als bedrohlich identifizierter Datenverkehr kann aus dem Gesamtverkehr gefiltert werden, ohne dass es zu einer Beeinträchtigung des legitimen Verkehrs kommt.

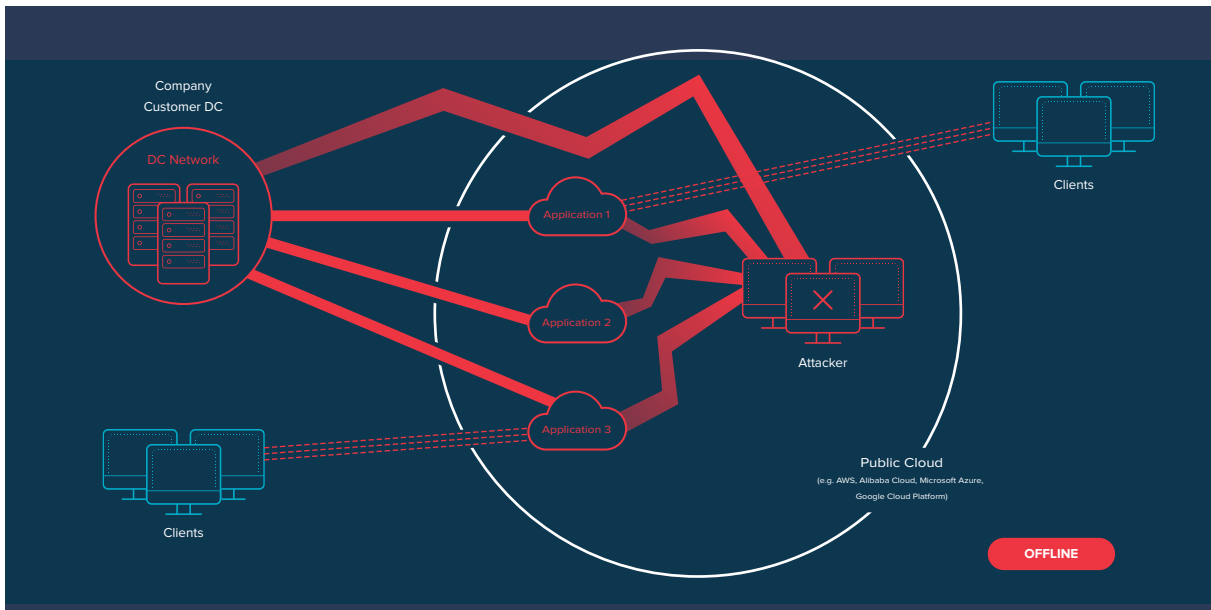
Die externen Cloud-Filter von Link11 arbeiten nach diesem Prinzip und ergänzen den Standard-Schutz der großen Cloud-Anbieter.

Mit den großen Cloudanbietern werden eigene Cross-Connects unterhalten. In externen Systemen erfolgt die Abarbeitung der Filterregeln ohne eine Einschränkung der dem Unternehmen zur Verfügung stehenden Bandbreite. So werden die potenziellen Schwachstellen eines vom Unternehmen aufgebauten Private Peering aufgehoben, weil die Filterung vollständig extern abläuft.

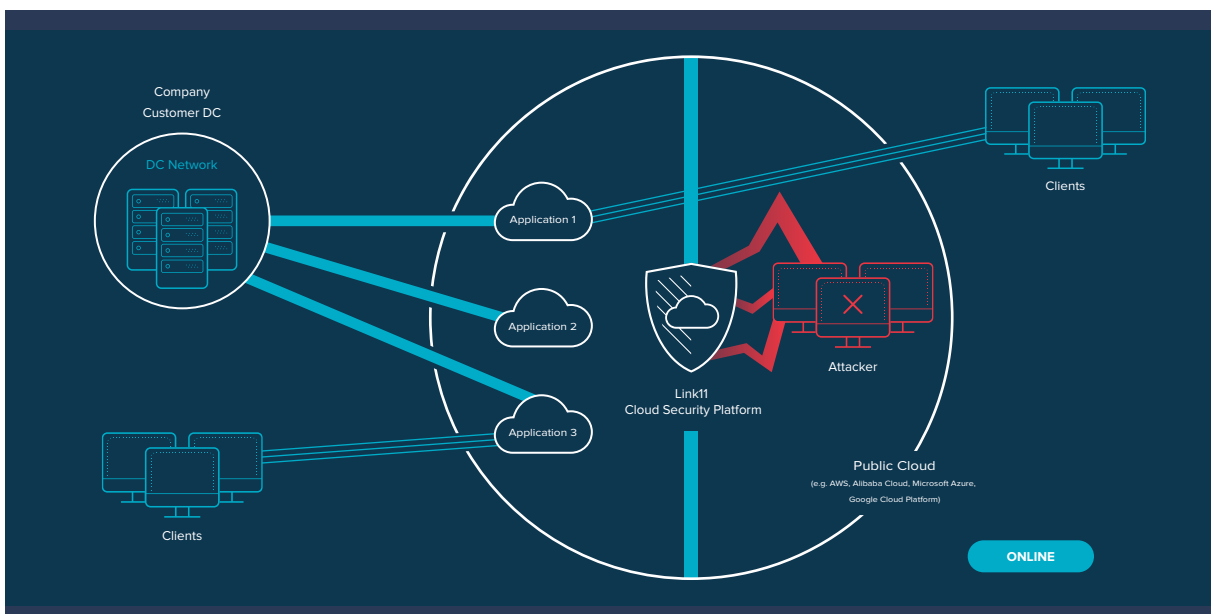
Dabei stehen die gleichen Vorteile anderer Cloud-Lösungen zur Verfügung. Der Schutz ist beliebig skalierbar und wird im akuten Angriffsfall angepasst. Gegenüber anderen Lösungen bietet sich beim Einsatz einer externen DDoS-Filterung ein weiterer Vorteil. Der WAN-Anschluss des Unternehmens muss nicht öffentlich gemacht werden. Er wird durch den vorgeschalteten Filter verschleiert. Weitere Attacken werden so verhindert bzw. erschwert.

DDoS-Angriffe aus der Cloud - wenn der Freund zum Feind wird

Nicht nur Wirtschaftsunternehmen haben die Vorteile der Cloud für sich entdeckt. Auch Kriminelle nutzen die modernen Cloudlösungen. Sie decken ihren Ressourcenbedarf an Instanzen und Bandbreite für DDoS-Angriffe über gehackte Accounts bei öffentlichen Cloud-Betreibern. Die Angriffe über missbrauchte Cloud-Instanzen können sich gegen alle Teile der hybriden IT-Infrastruktur eines Unternehmens richten.



Auch hier könnte man meinen, dass das Blockieren von Cloud-Services die einfachste Lösung zur Abwehr von DDoS-Angriffen aus der Cloud auf die Cloud ist. Da die Firmen häufig selbst diese Dienste nutzen, wäre somit auch die eigene Anbindung unterbrochen und Geschäftsprozesse kämen zum Stillstand. Die Filterung des DDoS-Angriffstraffics aus der Cloud über einen Cloud-Filter löst dieses Problem. So bleiben sowohl die cloud-basierten Services als auch die lokale Infrastruktur des Unternehmens erreichbar.



Fazit

Immer mehr geschäftskritische Prozesse landen in der Cloud. Die Zahl, der mit ihr verbundenen Apps und Geräte, wird in den kommenden Jahren noch weiter wachsen.

Dies erfordert aber nicht nur eine Strategie, die sich mit den betriebswirtschaftlichen Aspekten und der Prozessoptimierung beschäftigt. Unbedingt notwendig ist eine Sicherheitsstrategie, die auch neueste Bedrohungsszenarien berücksichtigt.

Unternehmen sollten deswegen auf externe Beratung zurückgreifen, um auszuloten, wie cloudbasierte Sicherheitslösungen dabei unterstützen, die Risiken aus Angriffen zu minimieren. KI-basierte Systeme versprechen hier wirkungsvollen Schutz, der deutlich über konventionellen Lösungen liegt.

Quellenangaben

¹KPMG und Bitkom: Cloud-Monitor 2019: Public Cloud und Cloud Security sind kein Widerspruch, Juni 2019

<https://hub.kpmg.de/cloud-monitor-2019>

²RightScale: 2019 State of the Cloud Report from Flexera, Februar 2019

<https://info.flexera.com/SLO-CM-WP-State-of-the-Cloud-2019>

³The Register: Amazon is saying nothing about the DDoS attack that took down AWS, but others are, Oktober 2019

https://www.theregister.co.uk/2019/10/28/amazon_ddos_attack/

⁴Link11: DDoS-Report 1. Halbjahr 2019, September 2019

<https://www.link11.com/de/downloads/ddos-report-1-halbjahr-2019/>

Über Link11

Link11 ist ein im Bereich Cyber Resilienz führender IT-Sicherheitsanbieter mit Hauptsitz in Deutschland. Die Schutzlösungen der Link11 Cloud Security Plattform sind vollständig automatisiert, reagieren in Echtzeit und werden durch KI-Algorithmen und maschinelles Lernen auch bei neuartigen Angriffen in unter 10 Sekunden ständig besser. Link11 bietet laut Gartner Report die schnellste time to mitigate (TTM), die auf dem Markt verfügbar ist. Um Cyber Resilienz zu gewährleisten, sorgen neben Web-DDoS- und Infrastructure-DDoS-Protection die Secure-DNS-, Zero Touch WAF (Web Application Firewall)-, Secure-CDN- und Threat-Intelligence-Services für eine ganzheitliche Härtung der gesamten IT-Infrastruktur und kritischer Anwendungen von Unternehmen auf Basis der integrierten Cloud-Security-Plattform. Die internationalen Kunden profitieren so von einem 360° Schutz und maximaler Performance.

Seit der Gründung des Unternehmens im Jahr 2005 wurde Link11 mehrfach für seine innovative Lösung und das starke Wachstum ausgezeichnet.