DER VERTRAUENSFAKTOR

Die Rolle der Cybersicherheit beim Aufrechterhalten der Geschäftsdynamik

Kurzfassung

Im Jahr 2018 war die Gefahr durch Cyberangriffe höher denn je. Aufsehenerregende Vorkommnisse rund um Datensicherheit machten weiter Schlagzeilen – unter anderem war darunter der größte jemals festgestellte DDoS-Angriff (Distributed Denial of Service) mit 1,7 Tbit/s.[1] In der Europäischen Union trat am 25. Mai 2018 die Datenschutz-Grundverordnung (DSGVO) in Kraft, die strenge neue Regeln dazu auferlegt, wie personenbezogene Daten zu erfassen, zu schützen und zu kontrollieren sind. Zudem traten Cryptominer auf den Plan, die Netzwerke infiltrierten, um schnellen Gewinn zu machen.

Wir leben in einem Zeitalter des Vertrauensverlusts – Unternehmen und Einzelpersonen nehmen Sicherheitsversprechen immer weniger für bare Münze. Bei Interaktionen mit Marken entscheiden Verbraucher jedes Mal neu, ob sie einem Unternehmen so sehr vertrauen, dass sie personenbezogene Daten übermitteln.
Erfolgreiche Cyberangriffe zerstören das Markenvertrauen, das Unternehmen durch harte Arbeit bei Kunden aufgebaut haben. Konsequenzen müssen nicht mehr allein die Sicherheitsexperten tragen – auch C-Level-Führungskräfte werden zur Rechenschaft gezogen.

Um Einblicke in die komplexen Herausforderungen zu vermitteln, vor denen Unternehmen im Kampf um den Schutz ihrer Marken stehen, gibt Radware jedes Jahr einen Global Application & Network Security Report heraus. Die aktuelle achte Ausgabe des Berichts kombiniert Resultate organischer Recherchen von Radware, reale Angriffsdaten sowie Analysen aufkommender Trends und Technologien mit den Ergebnissen einer weltweiten Branchenumfrage.

Der Bericht beleuchtet die geschäftlichen und technologischen Auswirkungen von Cybersicherheit. Unter anderem geht es dabei um folgende Themen:

- Lehren aus den jüngsten Angriffen
- Wahre Kosten von Cyberangriffen in quantitativer und qualitativer Hinsicht
- Übersicht zur Bedrohungslage bei Netzwerken und Applikationen
- Einsichten zu Schwachstellen bei aufkommenden Technologien
- Prognosen für 2019

WESENTLICHE ERGEBNISSE

Abwägung von Kosten und Risiken
Für den Schutz vor Cyberangriffen sind erhebliche Mittel erforderlich, die als Betriebskosten verbucht werden. Naturgemäß sind Unternehmen immer bestrebt, Kosten zu sparen. Wie viel sollte aber doch investiert werden angesichts des Risikos, dass Cyberangriffe die Verteidigungssysteme durchdringen und das Geschäft beeinträchtigen?

Werfen Sie dazu einen Blick auf diese Erkenntnisse aus der weltweiten Branchenumfrage 2018-2019 von Radware:

- Innerhalb nur eines Jahres stiegen die Anfangskosten, die Cyberangriffen zuzuschreiben sind, um 52 Prozent auf 1,1 Millionen US-Dollar.
- Kostenschätzungen der Unternehmen, in denen die von Cyberangriffen verursachten Gesamtkosten in einem Modell erfasst werden, sind fast doppelt so hoch wie Schätzungen anderer Unternehmen ohne Kostenmodellierung.
- Bei 40 Prozent der Unternehmen kam es nach einem erfolgreichen Angriff zu Beeinträchtigungen des Kundenservice und einem Reputationsverlust.
- 93 Prozent der Befragten haben in den vergangenen zwölf Monaten einen Cyberangriff erlebt; nur sieben Prozent sind vor Angriffen verschont geblieben.
- In einem Drittel der Unternehmen kamen Cyberangriffe wöchentlich vor.
- Hauptauswirkung von Cyberangriffen waren Dienstunterbrechungen, von denen fast die Hälfte der Befragten berichteten. Attacken, die zu einer vollständigen oder partiellen Dienstunterbrechung führten, nahmen um 15 Prozent zu und führten zu entsprechenden Produktivitätsbeeinträchtigungen.
- Cyber-Lösegeldforderungen, verbunden mit 51 Prozent der Angriffe, waren weiter die Hauptmotivation für Hacker.

[1] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/memcache-ddos-as-a-service/

Neue Angriffsvektoren

Angreifer setzen effiziente Verfahren ein, um Denials of Service zu verursachen – Beispiele sind Burst- oder Amplification-Angriffe, Verschlüsselungen oder IoT-Botnets im Internet der Dinge. Dabei wird gezielt die Applikationsebene ins Visier genommen, um größere Schäden zu verursachen.

- Angriffe auf Applikationsebene haben die meisten Schäden verursacht. Zwei Drittel der Befragten haben Angriffe auf Applikationen erlebt. Ein Drittel ist der Meinung, dass Sicherheitslücken bei Applikationen – insbesondere in Cloud-Umgebungen – 2019 großen Anlass zur Sorge geben werden. Über die Hälfte der Befragten haben Änderungen vorgenommen und Applikationen monatlich aktualisiert, während Updates bei den übrigen Unternehmen häufiger erfolgten, so dass automatisierte Sicherheitssysteme notwendig werden.
- Cyberangriffe, die zu einem vollständigen Ausfall oder einer Dienstunterbrechung führten, nahmen um 15 Prozent zu, und jedes sechste Unternehmen war bereits Ziel eines 1-Tbit/s-Angriffs.
- Hacker fanden neue Taktiken dafür, Netzwerke und Rechenzentren zusammenbrechen zu lassen: HTTPS-Floods nahmen um 20 Prozent zu, DNS- und Burst-Angriffe jeweils um 15 Prozent und Bot-Angriffe um 10 Prozent.
- In einem Drittel der Unternehmen kamen Angriffe vor, für die kein Motiv ausgemacht werden konnte.

Vorbereitung auf die Zukunft

In den Unternehmen ist man sich nach eigener Aussage bewusst, welche gravierenden Gefahren von der sich wandelnden Bedrohungslandschaft ausgehen. Entsprechend werden Maßnahmen ergriffen, um die eigenen digitalen Assets zu schützen. Dennoch stellt der Schweregrad der Sicherheitsbedrohungen eine große Belastung dar.

- Knapp die Hälfte der Befragten fühlten sich schlecht vorbereitet auf die Verteidigung gegen alle Arten von Cyberangriffen, obwohl in den jeweiligen Unternehmen Sicherheitslösungen zum Einsatz kommen.
- In 86 Prozent der Unternehmen hat man sich innerhalb der letzten zwölf Monate mit Lösungen beschäftigt, die auf maschinellem Lernen oder künstlicher Intelligenz basieren. Ziel war dabei in knapp der Hälfte der Fälle ein schnelleres Reagieren auf Cyberangriffe. Radware stellte beim geschäftlichen Einsatz der Blockchain-Technologie ein Wachstum von 44 Prozent fest.
- Unternehmen diversifizierten ihren Netzwerkbetrieb weiterhin durch Aufteilung auf mehrere Cloud-Provider. In 40 Prozent der Unternehmen kommen Hybridlösungen für Cybersicherheit zum Einsatz, die Schutz vor Ort mit cloudbasiertem Schutz verbinden.
- Befragte aus 49 Prozent der Unternehmen in der EMEA-Region gaben an, auf die DSGVO nicht gut vorbereitet zu sein.

Erfolg als einzige Option

Die durch Cyberangriffe verursachten Kosten sind so hoch, dass jede Bedrohung jedes Mal erfolgreich abgewehrt werden muss. Das Vertrauen von Kunden lässt sich binnen weniger Minuten zerstören – mit schwerwiegenden Auswirkungen auf die Markenreputation und hohen Kosten für das Wettmachen von Umsatzverlusten. Die Datenschutz-Grundverordnung und weitere gesetzliche Vorgaben können Unternehmen, die dagegen verstoßen, in Konkurs geraten lassen.

Für Unternehmen ist es entscheidend, Cybersicherheit in die langfristigen Wachstumspläne einzubeziehen. Der Schutz digitaler Assets darf nicht mehr allein an die IT-Abteilung delegiert werden. Die Sicherheitsplanung muss stattdessen in neue Produkt- und Serviceangebote, Sicherheits- und Entwicklungspläne sowie Geschäftsinitiativen einfließen. Der CEO muss gemeinsam mit dem Führungsteam den Ton angeben, damit in die Sicherung eines guten Kundenservice investiert wird.

Perspektiven des Top-Managements

CEOs als neue Vertrauensmanager

Cybersicherheit wird für Manager, denen man die Unternehmensführung auf höchster Ebene anvertraut hat, zu einem sehr persönlichen Thema. Um stabile Kundenbeziehungen aufzubauen und aufrechtzuerhalten, müssen CEOs eine zusätzliche Rolle als „Chief Trust Officer" ausfüllen. Wenn eine in jahrelanger Arbeit etablierte Markenstrategie durch einen einzigen Cyberangriff ausgelöscht werden kann, reicht es nicht mehr aus, dem Chief Information Security Officer (CISO) die Verantwortung für das Thema Sicherheit zu übertragen. Zu viel steht auf dem Spiel.

Denken Sie nur an das Schicksal von CEOs in Unternehmen wie Equifax, Yahoo, Moller-Maersk und Anthem Healthcare, bei denen bedeutende Sicherheitsverletzungen bekannt wurden. Die gesamte Arbeit, die in den Aufbau des Markenwerts geflossen war, wurde zunichte gemacht, als Kunden durch die Angriffe ihr Vertrauen verloren. Danach dauerte es nicht lange, bis die CEOs der meisten dieser Unternehmen „anderen Interessen nachgehen" durften.

Cybersicherheit muss ein fester Bestandteil des Geschäftsmodells sein. Deshalb ist es erforderlich, dass CEOs die entsprechenden Anstrengungen überprüfen und Mittel für Schutzmaßnahmen bereitstellen. CEOs, die ihre Sicherheitsstrategie ohne angemessene Kontrolle delegieren, tun dies auf eigene Gefahr.

Gratis herunterladen

Global Application & Network Security Report 2018–2019

Dieses Dokument wird ausschließlich zu Informationszwecken bereitgestellt. Die Fehlerfreiheit dieses Dokuments wird nicht garantiert, und das Dokument unterliegt keinerlei sonstigen Garantien oder Bedingungen, unabhängig davon, ob diese mündlich gegeben werden oder sich aus dem geltenden Recht ergeben. Radware schließt insbesondere jegliche Haftung für dieses Dokument aus. Durch dieses Dokument entstehen keine direkten oder indirekten vertraglichen Verpflichtungen. Die hier beschriebenen Technologien, Funktionen, Dienste und Prozesse können ohne Vorankündigung geändert werden.

© 2019 Radware Ltd. Alle Rechte vorbehalten. In diesem Dokument genannte Produkte und Lösungen von Radware sind durch Marken, Patente und Patentanmeldungen von Radware in den USA und anderen Ländern geschützt. Weitere Informationen finden Sie unter https://www.radware.com/LegalNotice/. Alle übrigen Marken und Namen sind Eigentum der jeweiligen Inhaber.