radware

GLOBAL APPLICATION & NETWORK SECURITY REPORT 2017-18

KURZFASSUNG

In den Schlagzeilen des Jahres 2017 waren Cyberangriffe und Sicherheitsbedrohungen vertreten, bei denen es um eine mögliche Beeinflussung der US-Präsidentschaftswahlen, um weltweite Malware-Epidemien und um den Equifax-Datendiebstahl ging. Diese und ähnliche bekannt gewordene Vorfälle haben zu höheren Investitionen in Cyberverteidigung geführt – bei staatlichen Stellen und globalen Konzernen, aber auch bei Privatpersonen, die Anti-Malware-Lösungen für ihre persönlichen Geräte erwarben. Dem Anstieg der Investitionen steht allerdings auch ein Anstieg der Bedrohungen, Hacks und Schwachstellen gegenüber.

Mit dem *Global Application & Network Security Report* verfolgt Radware das Ziel, diese komplexe und schwierige Dynamik besser zu verstehen. Der Bericht enthält die Ergebnisse einer weltweiten Branchenumfrage und Resultate organischer Recherchen von Radware. Zudem wurden reale Angriffsdaten und Kundenberichte verarbeitet – so entsteht ein Eindruck vom aktuellen Stand der Dinge und von den Handlungsmöglichkeiten in Sicherheitsabteilungen.

Die gesamte Security-Community kann von diesem Bericht profitieren, der die Radware-Untersuchungen und -Erkenntnisse zu den folgenden Themen darstellt:

- Bedrohungslandschaft – welche Angreifer gibt es, welche Motive haben sie und wie gehen sie vor?
- Potenzielle Auswirkungen auf Ihr Geschäft, einschließlich der mit verschiedenen Angriffsformen verbundenen Kosten
- Vorbereitungsgrad in unterschiedlichen Branchen
- Erfahrungen von Unternehmen in Ihrer Branche
- Neue Bedrohungen und wie Sie sich davor schützen können
- Prognosen für 2018

AM LIMIT

Auslöser von Cyberangriffen ist heutzutage meistens Cyberkriminalität. Angreifer streben finanzielle Vorteile an und wollen sich dafür den Erfolg von Kryptowährungen zunutze machen. Die Attacken werden unterdessen immer zielgerichteter. Ein entschlossener Feind nimmt sich Zeit für das Erkunden seines Angriffsziels und investiert in Ausspähung, Social Engineering sowie spezifische Hilfsmittel.

Als gängigste Angriffsvektoren sind Malware, Bots und Social-Engineering-Bedrohungen aufgekommen. Unternehmen sollten allerdings nicht nur die offensichtlichen Bedrohungen fürchten, sondern auch das, was sich schon als Gefahr abzeichnet, beispielsweise IoT-Botnets, Permanent Denial-of-Service (PDoS), SSL-basierte Angriffe und ausgeklügelte Malware-Injektionen. Zur Vorbereitung können sich Unternehmen mit neuen Technologien wie IoT, Blockchain und FaaS-Computing (Function-as-a-Service) bzw. Serverless Computing vertraut machen.

Vorschriften, etwa in Form von branchenbezogenen oder regionalen Richtlinien, spielen weiterhin eine wichtige Rolle beim Anheben der Sicherheitsstandards. Viele Unternehmen richten sich nach Sicherheits- und Datenschutzstandards, legen bei der Beurteilung von Sicherheitslösungen aber weniger großen Wert auf Compliance und Zertifizierungen. In einigen Unternehmen sind nicht einmal alle Zertifizierungen bekannt, und fast ein Drittel der Unternehmen erkundigen sich bei Anbietern niemals nach Zertifizierungen.

Massive weltweite Cyberangriffe waren 2017 einfach deshalb erfolgreich, weil es ungepatchte Schwachstellen gab: Ein kleiner, verbreiteter menschlicher Fehler hat verheerende Folgen. Als logische Lösung könnten insofern maschinelles Lernen oder künstliche Intelligenz (KI) infrage kommen. 20 Prozent der Unternehmen verlassen sich schon jetzt auf derartige Lösungen; weitere 28 Prozent planen die Implementierung für 2018. Derartige Lösungen sind jedoch nicht unfehlbar – man denke nur an die Risiken durch KI-Vergiftung sowie Manipulationen oder Fehler bei automatisierten Systemen (beispielsweise Microsoft Tay und Facebook-Chatbots).

Betrachtet man all das zusammengenommen, wird klar, dass wir vor einer gefährlichen Kluft stehen: Menschen nähern sich den Grenzen ihrer kollektiven Kontrollfähigkeit. KI und maschinelles Lernen sind jedoch noch nicht komplett ausgereift, sodass diese Ansätze leicht ausgetrickst werden können.

WEITERE ERGEBNISSE UND HIGHLIGHTS

Lösegeldforderungen bei jedem zweiten Angriff

Der in die Höhe schießende Bitcoin-Kurs hat auch eine starke Zunahme von Ransomware-Angriffen bewirkt. Unternehmen gaben an, dass bei der Hälfte aller Attacken Lösegeld gefordert wird. Lösegeldforderungen sind damit die Hauptmotivation für Angriffe – weit vor Bedrohungen durch Betriebsangehörige, Hacktivismus und Spionage seitens Mitbewerbern, um nur einige Beispiele zu nennen. Weltweit haben 42 Prozent der Befragten Ransomware-Angriffe erlebt; gegenüber 2016 ist das ein Anstieg um 40 Prozent.

Datendiebstahl als größte Sorge

Datendiebstahl/Informationsverlust führt die Liste der Sicherheitssorgen an – 28 Prozent der weltweit befragten Unternehmen verwiesen darauf. Mit 23 Prozent belegt die Angst vor Betriebsstörungen/ Ausfällen einen weiteren Spitzenplatz.

Zunahme bei DDoS-Angriffen speziell auf der Anwendungsebene

DDoS-Angriffe haben um 10 Prozent zugenommen; fast 40 Prozent der Unternehmen waren betroffen. Jedes sechste Unternehmen erlebte den Angriff eines IoT-Botnets, und 68 Prozent der Angriffe führten zu Performance-Einbußen oder einem Totalausfall – verbunden mit den entsprechenden Kosten. Angriffe auf Anwendungsebene legten 2017 im Vergleich zu Angriffen auf Netzwerkebene zu.

Keine Kostenerfassung bei 80 Prozent der Befragten

In 80 Prozent der Unternehmen werden die Kosten von Cyberangriffen nicht kalkuliert. Bei jedem dritten Unternehmen gibt es noch immer keinen Notfallplan, obwohl Cyberangriffe mittlerweile fast schon alltäglich sind. Erschreckenderweise folgt auf jeden vierten Angriff ein Kundenverlust oder eine Kundenklage gegen das betroffene Unternehmen.

Nach wie vor Handlungsbedarf in puncto Sicherheit

Fehlerhafte Sicherheitskonfigurationen (26 Prozent) und Sicherheitslücken bei Anwendungen (23 Prozent) wurden als höchste Risiken in Cloud-Umgebungen genannt. Die Befragten gaben auch an, dass 51 Prozent der Cloud-Anwendungen wöchentlich geändert werden (im Vergleich zu 2016 ist das ein Anstieg um 16 Prozent). Häufige Änderungen stellen in Bezug auf Transparenz und Kontrolle eine Herausforderung für die Sicherheitsverantwortlichen dar – besonders dann, wenn ein Viertel der Anwendungen unternehmenskritisch sind.

Die häufigsten Sicherheitsprobleme bei der Migration von Anwendungen in die Cloud sind Kontrolle, Governance und fehlende Transparenz; 46 Prozent der Unternehmen nennen diese Aspekte. Danach folgen fehlendes Know-how und die gestiegene Komplexität der Verwaltung von Sicherheitsrichtlinien. Interessanterweise nehmen 51 Prozent der Public-Cloud-Nutzer auch Sicherheitsdienstleistungen der Cloud-Provider in Anspruch, obwohl es sich dabei nicht immer um sicherheitsorientierte Unternehmen handelt.

Geblocktes Potenzial?

Blockchain-Technologie ist aktuell in aller Munde – 36 Prozent der Befragten gaben aber zu, dass sie den zugrunde liegenden Mechanismus nicht verstehen. Nur 10 Prozent sind der Meinung, dass Blockchain-Technologie die Informationssicherheit erhöhen wird.

Keine Qualifizierung der Bildungsbranche

Unter allen Branchen ist das Bildungswesen auf diverse Cyberangriffe am schlechtesten vorbereitet. Im zweiten Jahr in Folge liegt dieser Sektor auf dem letzten Platz.

Fehlende DSGVO-Vorbereitung bei 72 Prozent

Fast drei Viertel der Unternehmen (72 Prozent) sind nach eigener Einschätzung nicht gut vorbereitet auf die Datenschutz-Grundverordnung (DSGVO) der EU. Bei 16 Prozent dieser Gruppe war die DSGVO sogar gänzlich unbekannt.

Im jährlich erscheinenden *Global Application & Network Security Report* von Radware finden Sicherheitsteams Einblicke und Erkenntnisse, die das Analysieren der Bedrohungslandschaft und das Entwickeln von Sicherheitsstrategien zum Schutz der Unternehmen erleichtern. Cyberangreifer entwickeln ihre Zielauswahl, ihre Techniken und Angriffsvektoren beständig weiter – besuchen Sie deshalb DDoSWarriors.com, das Sicherheitscenter von Radware, um immer einen Schritt voraus zu bleiben.

© 2017 Radware, Ltd. Alle Rechte vorbehalten. Radware sowie alle anderen Produkt- und Dienstleistungsnamen von Radware sind eingetragene Marken von Radware in den USA und anderen Ländern. Alle übrigen Marken und Namen sind Eigentum der jeweiligen Inhaber. **www.radware.com**