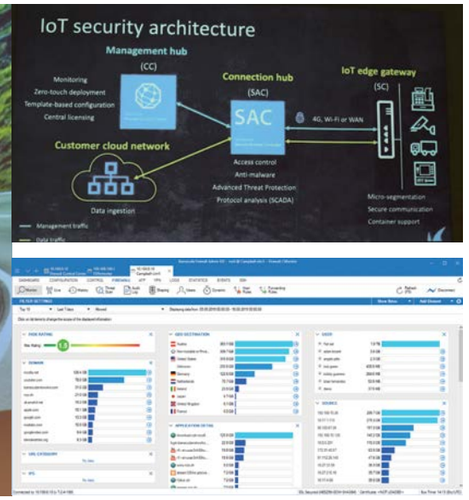
»Moderne Bedrohungen finden neue Wege, um E-Mail-Gateways zu umgehen. Unternehmen müssen neue Ansätze zur Prävention, Erkennung und Reaktion verfolgen«, lautete die Botschaft von Hatem Naguib in Alpbach.

»Wir werden uns im nächsten Schritt mehr der Maschinenvernetzung widmen«, kündigte Klaus Gheri an – bedingt durch den Faktor Kommunikation, der Teil jeder Maschine ist, durch den hohen Automatisierungsgrad und die automatisierten Konfigurationseinstellungen.



Für zuverlässigen Schutz in Multi-Cloud-Umgebungen sorgt die neue Version 8 der Barracuda CloudGen Firewall dank hohem Automatisierungsgrad und besserer Performance.

»Einfache Anwendung von komplexem Engineering«

Zum 15. Mal lud Barracuda zu seinem Tech Summit. Im malerischen Alpbach standen wieder Firewall, Anti Spam, Anti Phishing, cloudbasierte Backups und Cloud Security im Mittelpunkt

Karin Legat aus Alpbach

Der 360-Grad-Rundblick in die Tiroler Landschaft vor Betreten des Kongresscenters in Alpbach vermittelte vorerst Sicherheit und Wohlbefinden. Danach wurden die Besucher aber mit der Realität konfrontiert. IT-Sicherheit wird trotz täglicher Warnungen und Vorfälle weltweit noch immer zu wenig beachtet. Sicherheitsvorkehrungen in Unternehmen reichen häufig nicht aus, um Hackerangriffe abzuwehren. »2018 war für Barracuda ein *monumental year*«, berichtet COO Hatem Naguib dem *Telekom & IT Report*. Zahlreiche neue Produkte wurden auf den Markt gebracht. Das Motto dabei lautet »easy to buy, deploy and use«. Die einfache Anwendung auch von komplexem Engineering ist laut Naguib entscheidend – zu erfahren unter anderem bei der E-Mail-Protection und der CloudGen Firewall.

>> E-Mail-Schutz <<

Cyber-Angriffe gehören bereits zum Alltag vieler Unternehmen. Ein Großteil der Befragten bemerkt sie laut Deloitte jedoch erst spät oder gar nicht. 93 % der in einer Studie Interviewten aus mittleren und großen Unternehmen bestätigen dies. 25 % berichten von täglichen Angriffen, weitere 21 % haben ein- oder mehrmals pro Woche mit externen Attacken zu kämpfen.

Angreifer entwickeln ihre Taktiken laut Klaus Gheri, Vice President und General Manager Network Security bei Barracuda Networks, kontinuierlich weiter. Aktuell im Fokus: Lateral Phishing, bei dem gekaperte Nutzeraccounts für Phishing-Zwecke missbraucht werden. E-Mail-Sicherheit behält daher auch in den nächsten zwölf Monaten Priorität, gefolgt von Datenschutz und Netzwerksicherheit.

»Daten sind das neue Öl«, bestätigt Hatem Naguib in diesem Zusammenhang und zeigt auf, dass für viele Unternehmen das Auffinden, Identifizieren und Entfernen von E-Mail-Bedrohungen ein langsamer und manueller Prozess ist, der zu lange dauert und zu viele Ressourcen verbraucht. Laut einer aktuellen Umfrage des SANS Institutes nimmt die manuelle Behebung von Störfällen für 80 % der Unternehmen mehr als sechs Stunden in Anspruch. Die Lösung von Barracuda: Forensics and Incident Response. Damit kann automatisiert und proaktiv auf gezielte Angriffe reagiert werden, die an die Posteingänge der Benutzer gerichtet wurden. Die Plattform hilft, Anomalien in zugestellten E-Mails zu identifizieren.

>> Cloud-Ära <<

»Die Cloud ist auch in Europe die neue Normalität«, betonte Klaus Gheri. Aufgrund der wachsenden Cloud-Computing-Funktionen und -Services befinden sich zunehmend Daten an Stellen, wo herkömmliche IT-Sicherheitsmaßnahmen nicht mehr greifen, unter anderem in Datenzentren, die nicht zur eigenen IT-Gruppe gehören. Mit der neu am Markt verfügbaren CloudGen Firewall 8 bietet Barracuda eine Sicherheitslösung, die speziell für On-Premises, Cloud- und Hybridnetzwerke entwickelt wurde. Netzwerksegmentierung, Sicherheitseinstellungen sowie Zugriffskontrollen von IT-Ressourcen können im Rahmen agiler Cloud-Entwicklungsprozesse automatisch bereitgestellt werden. Damit lassen sich Verbindungen zwischen mehreren Standorten vor Ort und der Cloud sicher und zuverlässig einrichten. Die CloudGen Firewall kombiniert Next-Generation Security, leistungsstarke SD-WAN-Funktionen und einfache zentrale Verwaltung für hunderte oder tausende von Firewalls. IPS, URL-Filtering, dualer Virenschutz und Applikationskontrolle erfolgen verzögerungslos direkt im Datenfluss. Ressourcenintensivere Schutzmechanismen zur Abwehr von Ransomware durch Sandboxing sind in der Cloud integriert. Die CloudGen Firewall ist automatisch verbunden mit Azure vWAN inklusive zentraler Verwaltung, Zero Touch Deployment und Unterstützung von Office 365 vWAN-Richtlinien.

Vielfach fehlt das Vertrauen zu einer sicheren Cloud-Umgebung. Dem begegnet Barracuda mit seinem Cloud Security Guardian, der einen umfassenden Einblick in die Sicherheitslage von Public-Cloud-Workloads bietet, die kontinuierliche Compliance sicherstellt und die Behebung von Sicherheitsvorfällen automatisiert. Mithilfe der Security Graph-API von Microsoft werden Sicherheitsbewertungen und Warnungen bereitgestellt, um Verstöße gegen Sicherheitsrichtlinien zu identifizieren und zu verhindern. Cloud Security Guardian lässt sich auch in die Azure-Firewall von Microsoft integrieren.

Die Software ist mit auf CIS-Benchmarks basierenden Sicherheitsrichtlinien vorinstalliert und von CIS zertifiziert. Zu den wichtigsten Funktionen gehören eine interaktive Karte der Cloud-Ökosysteme eines Unternehmens, vereinfachte Drilldowns und Beziehungs-IDs sowie die automatische Behebung von Verstößen gegen Sicherheitsrichtlinien. ■

Die manuelle Behebung von Störfällen dauert für 80 Prozent der Unternehmen mehr als sechs Stunden. *(SANS)*

Problem der Fehlkonfigurationen

■ DIE ZUNEHMENDE MIGRATION der IT-Infrastruktur in die Cloud stellt eine wachsende Herausforderung an Sicherheit. 38 Prozent der Channelpartner von Barracuda berichten von Problemen ihrer Kunden, die Multi-Cloud-Umgebungen regelkonform zu halten, 51 Prozent von einem fehlenden vollständigen Überblick über die Sicherheit aller Endpunkte in der Multi-Cloud-Infrastruktur. 88 Prozent sind besorgt über die rasante Zunahme von Fehlkonfigurationen ihrer Kunden, die zu Sicherheitsrisiken führen.

Geteilte Verantwortung

■ »MIT DER CLOUD kann ich eine Sicherheit erreichen, wie sie nur schwer darstellbar ist, wenn ich sie selber gestalte. Oft werden Kompromisse geschlossen«, gibt Klaus Gheri zu bedenken. Mit der Cloud können Aufgaben an Organisationen, deren Kernaufgabe IT-Sicherheit ist, delegiert werden. Unternehmen müssen sich allerdings überlegen, welche Daten für die Cloudnutzung geeignet sind. »Die meisten Kunden unterscheiden sehr genau, was sie in der Cloud machen«, so Gheri und verweist auf das geteilte Verantwortungsmodell, das vielfach nicht bedacht wird. »Die Cloud betreibt die eigenen Rechenzentren sehr sicher, aber der Zugriff liegt im Verantwortungsbereich der Anwender und hier treten vielfach erhebliche Einbußen bei der Sicherheit auf.«

Fotos: Barracuda Networks, Pressebüro Legat