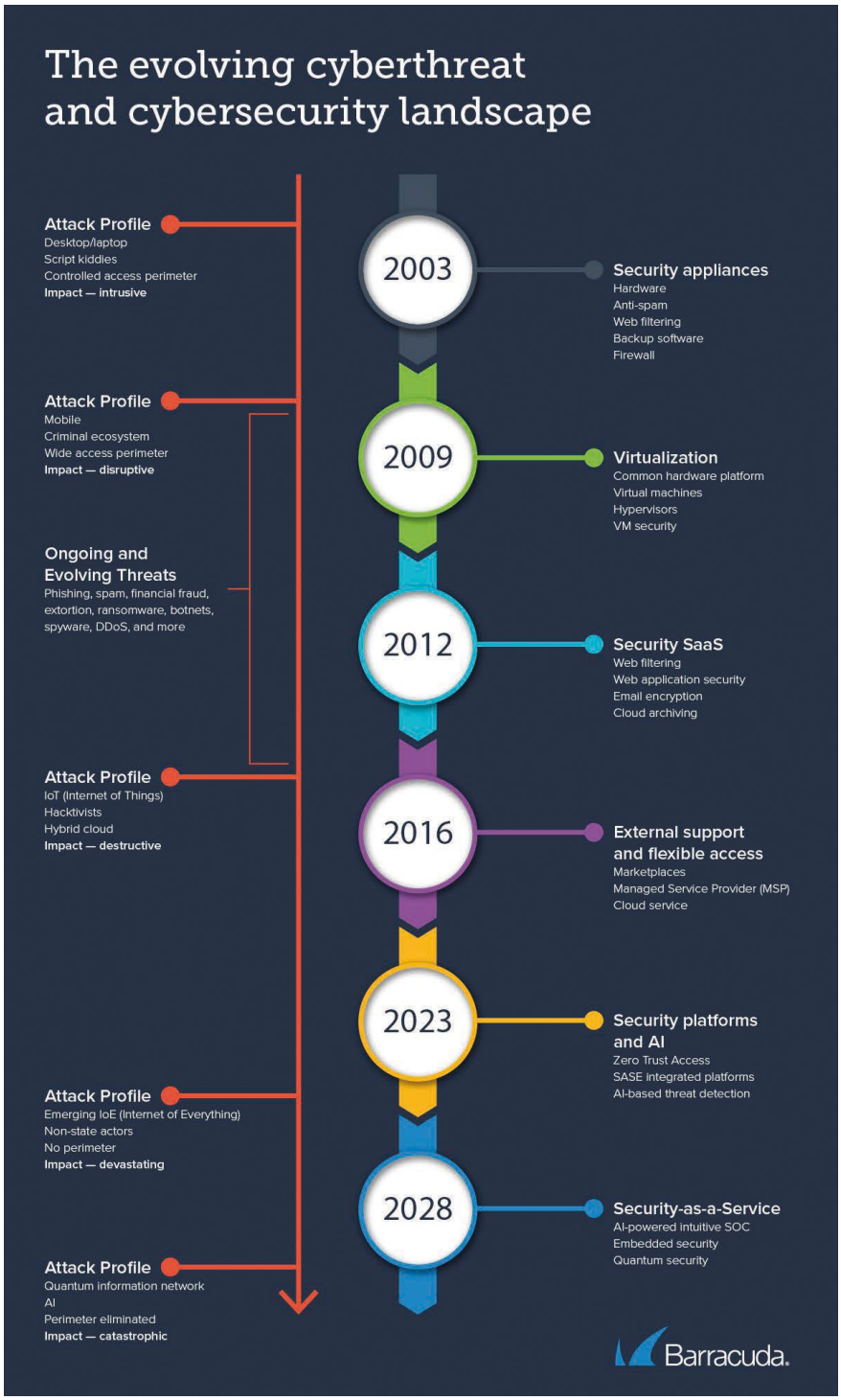
Eine kleine Geschichte der Cyberangriffe und deren Abwehr

Wie Angreifer und Verteidiger voneinander lernen



Autor:
Adam Khan, VP Global Security Operations, XDR
Barracuda Networks
www.barracuda.com

Seit mehr als 30 Jahren liefern sich Cyber-Angreifer und Sicherheitsteams einen Kampf in der digitalen Landschaft. Die eine Seite sucht nach Lücken und Schwachstellen, die sie ausnutzen kann, die andere Seite repariert und schützt sie. Das Tempo des Konflikts beschleunigt sich. Heute gibt es mehr als 1 Milliarde bekannter Malware-Programme. Davon sind 94 Millionen in den letzten 12 Monaten erschienen. Im Jahr 2009 lag die jährliche Zahl bei 25 Millionen.

Im Folgenden möchten wir einen Blick darauf werfen, wie sich Cyberangriffe und Cybersicherheit seit unseren Anfängen im Jahr 2003 entwickelt haben, und was uns in Zukunft erwarten könnte.

Die Bedrohungslandschaft im Jahr 2003

Cyberbedrohungen und die Cybersicherheit zur Abwehr dieser Bedrohungen kamen Mitte der 1980er Jahre auf. Der Cascade-Virus 1987/88, der Morris-Wurm 1988, der Melissa-Virus 1999, um nur einige zu nennen.

Bis 2003 begannen sich die Cyber-Bedrohungen zu diversifizieren und zu vervielfältigen, aber die Angriffe blieben weitgehend fragmentiert, störend und oft opportunistisch. Viren, Würmer und andere Malware machten sich die zunehmende Nutzung des Internets durch Unternehmen zunutze, wurden aber nicht wirklich als Teil organisierter cyberkrimineller Angriffskampagnen eingesetzt. Die Angriffe zielten auf Laptops und Desktop-Geräte ab und suchten nach Schwachstellen in einem definierten und kontrollierten Zugangsperimeter.

Suchen bekannter Malware

Die entsprechende Cybersicherheitslandschaft konzentrierte sich auf das Scannen nach bekannter Malware und deren Erkennung anhand von Signaturen sowie auf das Blockieren von Spam, Viren und einfachen Webangriffen. Das statische Signaturerkennungssystem wurde bald durch heuristische Erkennung (Erkennung von Viren durch Untersuchung des Codes auf verdächtige Eigenschaften) ergänzt, um die wachsende Zahl bisher unbekannter Malware-Varianten zu erkennen.

In den Startlöchern stand jedoch das erste Push-fähige BlackBerry-Handgerät, das 2002 auf den Markt kam und Mitarbeiter und Daten aus der traditionellen Enge des Arbeitsplatzes befreite. Es dauerte nicht lange, bis andere Geräte, Technologien und Anwendungen folgten, und alles änderte sich für immer.

Blick bis 2009

Bis 2009 eroberten mobile Geräte, Dienste und Software die Unternehmenslandschaft. Die Sicherheitsgrenzen dehnten sich immer weiter aus, und die Angreifer organisierten sich. Finanzbetrug, Phishing, Ransomware, Spyware, Botnets und Denial-of-Service-Angriffe (DoS und DDoS) traten in das Ökosystem der Cyberbedrohungen ein - und blieben dort. Einige der Angriffstaktiken, über die in dieser Zeit erstmals berichtet wurde, wie z. B. SQL-Injection, werden auch heute noch eingesetzt.

Um größere und vielfältigere digitale Arbeitslasten zu bewältigen, wurden virtuelle Maschinen (VM) und Vir-

tualisierung zu integralen Bestandteilen von IT-Netzwerken. In einer virtualisierten Umgebung kann es schwieriger sein, den Überblick über die Arbeitslasten und Anwendungen zu behalten, da sie zwischen den Servern wandern, was die Überwachung von Sicherheitsrichtlinien und -konfigurationen erschwert. Unzureichend geschützte virtuelle Maschinen können mit Malware infiziert werden und diese in der gesamten virtuellen Infrastruktur verbreiten. Die Virtualisierung bietet auch einige Sicherheitsvorteile. Wenn eine VM vom größeren Netzwerk isoliert ist, kann sie für Malware-Analysen, Penetrations- und Szenario-Tests verwendet werden.

Blick bis 2012

Das Zeitalter der modernen Ransomware war angebrochen. Webbasierte und Social-Engineering-Angriffe waren weit verbreitet, und die Angriffe von staatlich unterstützten Gruppen und Aktivisten nahmen zu.

Gleichzeitig trieb der Bedarf der Unternehmen an skalierbarer, zugänglicher Sicherheit, die in Echtzeit aktualisiert werden kann und keine Ressourcen verbraucht, die Sicherheit in die Cloud und in As-a-Service-Modelle. Unternehmen suchten außerdem nach Sicherheitslösungen, die ihre wachsenden Mengen an in der Cloud gehosteten Daten speichern und schützen können, sowie nach fortschrittlicher E-Mail-Sicherheit, um die immer raffinierteren E-Mail-basierten Angriffe abzuwehren.

Blick bis 2016

Im weiteren Verlauf des Jahrzehnts wurden Cyberangriffe immer häufiger und zerstörerischer. Vernetzte Internet-of-Things (IoT)-Systeme und hybride Cloud-/Orts-IT-Umgebungen wurden üblich und boten Angreifern eine breitere Angriffsfläche und neue Schwachstellen, die sie gezielt ausnutzen konnten. Angreifer nutzen dateilose Malware und legitime oder integrierte IT-Tools, um Sicherheitsmaßnahmen und Erkennung zu umgehen.

Viele Unternehmen waren mit den Fähigkeiten und Ressourcen, die für die Absicherung komplexer digitaler Umgebungen gegen solche Bedrohungen erforderlich waren, überfordert und wendeten sich daher vermehrt an Managed Service Provider, um externe Unterstützung zu erhalten. Das Sicherheitsangebot wurde flexibler und über die großen Online-Marktplätze und andere Dienstleister verfügbar, so dass es innerhalb weniger Minuten gekauft und in Betrieb genommen werden konnte.

Das Jahr 2017

2017 sollte ein entscheidendes Jahr für Cyberbedrohungen und Cybersicherheit werden. Es war das Jahr, in dem das leistungsstarke Exploit-Tool EternalBlue, das auf das SMB-Protokoll abzielt, veröffentlicht wurde, und es war das Jahr zweier Angriffe mit enormen globalen Auswirkungen - WannaCry und NotPetya.

Blick bis 2023

Wir sehen heute, wie sich das Internet zum Internet der Dinge (IoT) entwickelt. Sicherheitsintegration und -transparenz können damit nur schwer Schritt halten - was zu Sicherheitslücken führt, die Angreifer schnell ins Visier nehmen und ausnutzen.

Sowohl Angreifer als auch Verteidiger machen sich KI und maschinelles Lernen zunutze - erstere, um immer überzeugendere Social-Engineering-Angriffe und Malware zu entwickeln, letztere, um immer intelligentere Sicherheitstools zu entwickeln, die diese erkennen und blockieren.

Da Malware-Tools und -Infrastrukturen in großem Umfang als Service zur Verfügung stehen, sind Cyberangriffe für immer mehr Kriminelle erreichbar, was die Verbreitung von Ransomware, Erpressung und mehr begünstigt - und Unternehmen mit vielen Nutzern, Geräten, Anwendungen und Daten ins Visier nimmt, die weit über den einstigen Sicherheitsbereich hinaus aktiv sind.

Die Sicherheitsbranche hat sich angepasst und End-to-End-Netzwerksicherheitsplattformen eines einzigen Anbieters implementiert, die fortschrittliche Sicherheit bis an den Rand des Netzwerks bringen - bekannt als Secure Access Service Edge (oder SASE) - mit Zero-Trust-basierten Zugangskontrollen, Bedrohungsdaten, Reaktion auf Vorfälle und 24/7-Sicherheitszentren.

Der Russland-Ukraine-Krieg, der 2022 begann, hat die Welt auch daran erinnert, wie Cyberangriffstaktiken wie DDoS, Wipers und mehr in Zeiten geopolitischer Spannungen als Cyberwaffen eingesetzt werden können.

Blick bis 2028 – Wie sieht die Zukunft aus?

Auf dem Weg in die zweite Hälfte dieses Jahrzehnts wissen wir, dass Sicherheitsgrenzen der Vergangenheit angehören und dass Angriffe eher katastrophale Folgen haben werden, einfach weil wir so abhängig von riesigen, miteinander verbundenen digitalen Systemen und Infrastrukturen geworden sind. Die Sicherheit muss tief in diese Systeme eingebettet werden.

Wir gehen davon aus, dass sich der Einsatz von KI auf breiter Front fortsetzen wird, mit erheblichen Auswirkungen auf Unternehmen, Gesellschaft und geopolitische Stabilität. KI wird es den Sicherheitszentralen ermöglichen, intuitiv und reaktionsschnell zu werden und die Erkennung, das Verständnis und die Eindämmung komplexer Vorfälle zu beschleunigen.

Quantencomputing

Es wird erwartet, dass das Quantencomputing bis zum Ende des Jahrzehnts kommerziell nutzbar wird und alle Bereiche von der Arzneimittelentwicklung und den Finanzmärkten bis hin zum Klimawandel und zur Wettervorhersage verändern wird. Das Quantencomputing wird auch erhebliche Auswirkungen auf die Cybersicherheit haben, einschließlich der Fähigkeit, herkömmliche Verschlüsselungen zu knacken.

Schlussfolgerung

Cybersicherheit ist eine Reise. Ein Rückblick auf die letzten 20 Jahre zeigt uns, dass sich Angreifer und Sicherheitsteams kontinuierlich an die sich verändernde Landschaft und aneinander angepasst haben, wobei beide Seiten den Wandel vorantreiben und von ihm angetrieben werden. In den kommenden Jahren wird sich das Tempo der Veränderungen fortsetzen und beschleunigen. Es wird neue Schwachstellen und neue Bedrohungen geben, neben jahrzehntealten Taktiken und Schwachstellen - die Sicherheit muss auf all das vorbereitet sein. ◄