Das ändert alles: Ransomware im Zeitalter der KI

Barracuda

Der Aufstieg der generativen KI

Künstliche Intelligenz (KI) sorgt 2023 fast täglich für Schlagzeilen. Die Entwicklungen der generativen KI-Tools (GenAI) wie ChatGPT, Bard, Midjourney und anderen werden von Technologie-Gurus ebenso wie von Laien gepriesen. Jetzt steht GenAI im Mittelpunkt und wir dürfen nicht vergessen, dass KI zwar für positive Aktivitäten wie die Produktivität am Arbeitsplatz eingesetzt werden kann, aber auch für unheimlichere Zwecke. Ransomware ist einer der Bereiche, in denen KI von böswilligen Akteure für einen neuen und schädlichen Einsatz genutzt wird.

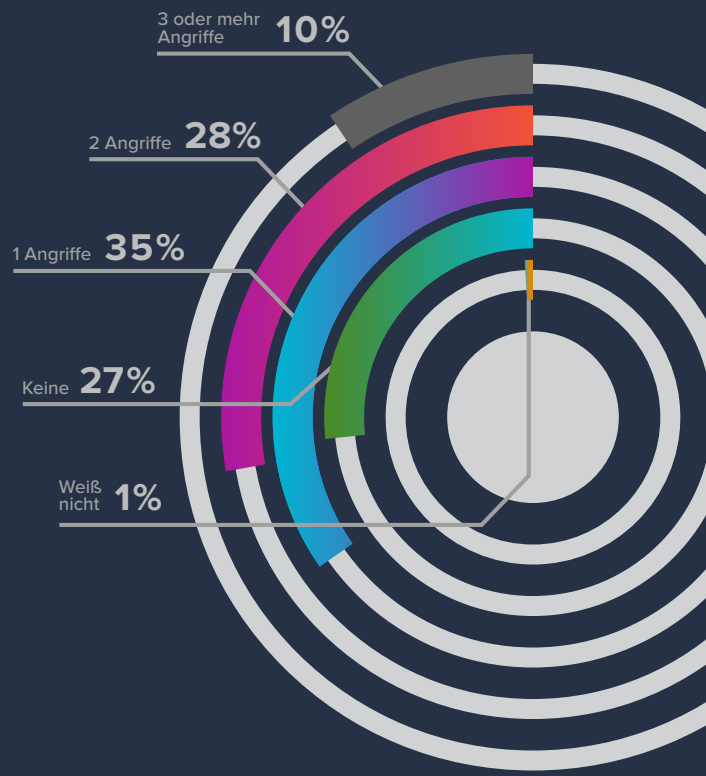
Barracuda

Die heutige Ransomware-Landschaft

Heutzutage breitet sich Ransomware massenhaft aus. Ransomware ist bösartige Software, die von Cyberkriminellen entwickelt und eingesetzt wird, um das Netzwerk ihres Ziels zu infizieren, Systeme außer Betrieb zu setzen und Daten zu verschlüsseln. Ransomware zielt darauf ab, sensible oder vertrauliche Informationen zu stehlen und damit zu drohen, die Daten zu veröffentlichen, wenn kein Lösegeld gezahlt wird. In 53 % von Ransomware-Fällen greifen Angreifer sensible Daten ab und verlangen zusätzliches Lösegeld, damit wertvolle Daten nicht öffentlich aufgedeckt werden. Die Einstiegshürden für Ransomware-Angriffe waren noch nie so niedrig und die Gewinne noch nie so hoch – es handelt sich um eine außerordentlich gewinnbringende Form von Cyberkriminalität mit geringem Risiko, die jedes Jahr mit zunehmender Raffiniertheit und Häufigkeit verübt wird.

Aus dem jüngsten Marktbericht von Barracuda, 2023 Ransomware-Einblicke, geht hervor, dass fast drei Viertel (73 %) der Befragten in 2022 von einem erfolgreichen Ransomware-Angriff betroffen waren und 38 % sogar mehr als einmal.

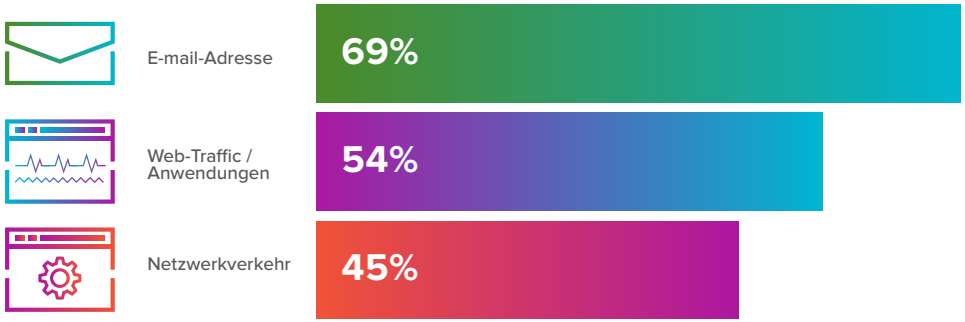
Wie viele erfolgreiche Ransomware-Angriffe haben Unternehmen in den letzten 12 Monaten erlebt?



Quelle: 2023 Ransomware-Einblicke

Die Ergebnisse zeigen außerdem, dass in 69 % der befragten Unternehmen einige der Ransomware-Angriffe, die sie erlebt haben, mit einer bösartigen E-Mail anfingen. Bei den größeren Unternehmen – mit mehr als 250 Mitarbeitenden – war der Prozentsatz mit 75 % sogar noch höher. Dies sind häufig Phishing-Angriffe, bei denen eine E-Mail mit einem bösartigen Link als echte E-Mail eines Unternehmens getarnt ist, in der die kompromittierte Person beispielsweise aufgefordert wird, ihre Zugangsdaten einzugeben, um ein Passwort zurückzusetzen, oder eine ähnliche Aktivität durchzuführen.

Manchmal lädt der Link in Phishing-E-Mails automatisch eine bösartige Datei herunter und führt sie aus, beispielsweise einen Key-Logger, so dass im Laufe der Zeit Zugangsdaten gestohlen werden können. Zugangsdaten sind der Schlüssel zur Infiltration des Netzwerks, um den Angriff voranzutreiben.



Quelle: 2023 Ransomware-Einblicke

In einigen Fällen gingen die ersten Angriffe nicht von E-Mails aus. Kunden, die mehr als einen Angriff erlebt haben, wurden häufig von mehreren Vektoren angegriffen. In demselben Bericht über Ransomware-Einblicke wurde in 54 % der gemeldeten Fälle angegeben, dass sie einen Erstangriff über ihre Web-Applikation erlebt hatten und in 45 % der Fälle erfolgte der erste erfolgreiche Angriff über das Netzwerk des Unternehmens. In den meisten Fällen verwenden die Angreifer eine Kombination aus Techniken, um Schwachstellen vollständig auszunutzen und den größten Nutzen aus dem Angriff zu ziehen.

Unabhängig vom Ursprung des Angriffs ist das Endziel, sich lateral auf der Suche nach abzugreifenden Daten durch das Netzwerk zu bewegen und die Voraussetzungen für einen Ransomware-Angriff zu schaffen. Nachdem die Daten gestohlen wurde, versuchen die Angreifer häufig, Backup-Daten zu verschlüsseln oder zu löschen, um eine Wiederherstellung zu verhindern, bevor sie die eigentliche Ransomware-Foderung starten.

KI-gestützte Ransomware

KI-gestützte Ransomware ist genau das, wonach es klingt: eine Kombination aus herkömmlicher Ransomware und neuen KI-Technologien. Cyberkriminelle setzen KI ein, damit ihre Ransomware-Angriffe effektiver sind und um die Produktivität ihrer Organisation zu steigern. Wir werden KI in allen Formen von Ransomware erleben: vom Phishing bis zur Aushandlung von Lösegeld-Beträgen.

KI und Automatisierung können zur Erstellung von Phishing-, Vishing- (Sprachphishing über das Telefon) und Smishing-Nachrichten (SMS-basiertes Phishing) eingesetzt werden. Sie können Netzwerkangriffe und Anwendungsangriffe starten, optimieren, wie das Abgreifen von Daten im normalen Datenverkehr versteckt werden kann, ebenso wie Ransomware-Beträge recherchieren und aushandeln – was auch immer es ist, KI wird da sein, um es zu optimieren. Das ist nichts, was man erst in der Zukunft erwarten kann. Es geschieht bereits jetzt und ermöglicht es Ransomware-Angriffen, neue Höhen zu erreichen, wie die neuesten Zahlen aus unserem eigenen Ransomware-Bericht zeigen.

Durch KI-erweiterte Phishing-Angriffe sind vielleicht das erste Beispiel dafür, wie bösartige Akteure diese neuen Funktionen einsetzen. Sobald ein Tool wie ChatGPT veröffentlicht wird, versuchen Cyberkriminelle, es auf innovative Weise für ihre eigenen schädlichen Zwecke zu nutzen. Dank GenAI-Chatbots und anderen Tools zur Verarbeitung natürlicher Sprache (NLP), die große Sprachmodelle (LLMs) verwenden, um Text zu generieren, der klingt, als wäre er von einem Menschen geschrieben worden, können Cyberkriminelle Nachrichten für Phishing-Links erstellen, ohne Tippfehler, Grammatikfehler und andere verräterische Anzeichen dafür, dass die E-Mail, SMS oder andere Kommunikation vielleicht nicht echt ist. Nicht-Muttersprachler können KI nutzen, um Nachrichten in anderen Sprachen generieren, ohne befürchten zumüssen, dass ihre Ausdrucksweise ihre falsche Identität preisgibt. Das bedeutet, die Zahl der Cyberkriminellen, die überzeugende Angriffe koordinieren können, hat sich drastisch erhöht ist und die Phishing-, Smishing- und Vishing-Nachrichten sind viel schwieriger zu identifizieren als bösartige.

Angreifer werden besser ausgerüstet sein, Netzwerk, Anwendung und andere IT-Schwachstellen zu finden und auszunutzen, da die KI einen Großteil der Arbeit für sie mit Aufforderungen in natürlicher Sprache übernimmt – fortgeschrittene Programmierkenntnisse sind nicht erforderlich. Zu diesem Zeitpunkt erfordert die KI noch eine gewisse Steuerung durch eine sachkundige Person, aber es besteht kein Zweifel daran, dass KI und Automatisierung für diese kriminellen Gruppen aufgrund der schieren Menge an Angriffen, die sie in hoher Geschwindigkeit initiieren können, von entscheidender Bedeutung sind.Auch Ransomware-as-a-Service (RaaS) wird dadurch beschleunigt, da individuell angepasste Angriffe wesentlich kostengünstiger ausgeführt werden können.

Wie man sich vor KI-gestützter Ransomware schützt

Barracuda empfiehlt einen Schutzansatz in drei Schritten, um ihr Unternehmen auf KI-basierte Ransomware-Angriffe vorzubereiten und davor zu schützen.

Das sind die wesentlichen Schritte:

1. **Schützen Sie Ihre E-Mails**
2. **Sichern Sie Ihr Netzwerk und Ihre Anwendungen**
3. **Sichern Sie Ihre Daten**

Der Schutz Ihrer E-Mails ist eine mehrstufige Übung. Unternehmen müssen sicherstellen, dass ihre E-Mail-Sicherheitslösung auch Zugangsdaten schützt, Schulungen mit einbezieht, die KI nutzen, um Defizite und besonders anfällige Personen zu identifizieren, und dass sie ein Security Operations Center (SOC) verwenden, um Anomalien zu erkennen.

Schulungen zur Stärkung des Risikobewusstseins (SAT) sind unverzichtbar – es ist wichtig, dass Ihre Mitarbeitenden verstehen, wie sie potenzielle Phishing-Angriffe identifizieren können und genau wissen, was zu tun ist, wenn sie glauben, dass sie kompromittiert wurden. Dies ist kein einmaliger Ansatz: Die Schulungen müssen regelmäßig erfolgen und auf den aktuellen Trends der Cyberangriffe basieren.

Der Schutz Ihres Netzwerks und Ihrer Anwendungen ist ebenfalls ein vielfältiges Unterfangen, für das wir ein ganzes anderes E-Book benötigen würden, um dies ausreichend zu behandeln. Die Grundlagen sind: Verwenden Sie Zero Trust Network Access (ZTNA), mit dem Sie einschränken, wer Zugriff auf Teile des Netzwerks und verschiedene Anwendungen hat. Segmentieren Sie Ihr Netzwerk und verwenden Sie Ihr SOC und erweitere Reaktion auf Erkennung (XDR), um ungewöhnlichen

Netzwerkverkehr zu erkennen. Schützen Sie Endpunkte, E-Mails, Firewalls, Server usw. Secure Access Service Edge (SASE) ist eine großartige Möglichkeit, um sicherzustellen, dass sowohl Ihre Cloud-Architektur als auch Ihre lokale Architektur zusammenarbeiten und mit dem effektivsten und effizientesten Maß an Security geschützt sind.

Die Sicherung Ihrer Daten ist ein weiteres entscheidendes Element zur Abwehr von Ransomware. Da Ransomware-Angriffe darauf abzielen, Ihre Systeme abzuschalten und Ihre Daten zu verschlüsseln, müssen Organisationen sicherstellen, dass sie ein unveränderliches, sicheres Backup ihrer Daten haben, damit sie diese wieder herstellen können, ohne Lösegeld zu zahlen.

Dieses Backup sollte über mehrere Eben von rollenbasierte Zugriffskontrollen verfügen, um sicherzustellen, dass nur die erforderlichen Personen Zugriff darauf haben. Es sollte auch getrennt vom Hauptnetzwerk gehalten werden, damit die Ransomware-Angreifer es im Falle eines Angriffs nicht finden und das Backup verschlüsseln können, um eine Wiederherstellung zu verhindern.

Wie KI hilft, Sicherheitsverletzungen zu verhindern und zu beheben

So wie KI von bösartigen Akteuren genutzt werden kann, um Ransomware-Angriffe einzuleiten, kann sie auch von den Security-Teams der Unternehmen verwendet werden, um dazu beizutragen, dass sie vor Verstößen geschützt sind und versuchte oder erfolgreiche Angriffe zu beheben:

- KI-gestützte Ransomware-Erkennung kann den Netzwerkverkehr, den Dateizugriff und Aktivitäten analysieren, die bedeuten könnten, dass ein Ransomware-Angriff entweder erwartet wird oder bereits im Gange ist.

- KI-gestützte Aktivitätsüberwachung kann das Benutzerverhalten untersuchen, um zu identifizieren, ob die Aktivität verdächtig ist oder wie gewohnt verläuft – zum Beispiel erfolglose Anmeldeversuche und ungewöhnlicher Dateizugriff.

- Die Multifaktor-Authentifizierung (MFA) kann mit KI verbessert werden, um die Security einer Organisation zu verstärken, indem die Tippgeschwindigkeit analysiert wird, mehrere Authentifizierungsebenen für sensible Daten verlangt werden und Benutzer gesperrt werden, die einen atypischen Zugriffsversuch unternehmen.

Fazit

Mit der Weiterentwicklung von KI-Ransomware-Angriffen werden auch die KI-Tools weiterentwickelt, die zum Schutz vor diesen Angriffen und zu ihrer Eindämmung entwickelt werden. Es ist wichtig, dass Unternehmen über alle neuesten technologischen Lösungen auf dem Laufenden bleiben, die dazu beitragen, diese schwerwiegenden, ausgeklügelten Verstöße zu verhindern und zu beheben. Der oft zitierte Grundsatz „Wenn man sich nicht vorbereitet, bereitet man sich auf das Scheitern vor“ trifft hier zu: Es ist wesentlich effizienter, sich auf Ransomware vorzubereiten und diese zu verhindern, als zu versuchen, einen erfolgreichen Angriff abzuwehren – und auch weniger kostspielig.

Wir hoffen, dass dieses E-Book dazu beiträgt, hervorzuheben, wie wichtig es ist, KI-gestützte Ransomware-Angriffe ernst zu nehmen und Methoden zu ihrer Verhinderung festzulegen, ebenso wie die dafür verfügbaren KI-Tools zu nutzen.

Die Ransomware-Lösung von Barracuda verfolgt einen dreistufigen Ansatz, um Sie vor allen Ransomware-Angriffen zu schützen, einschließlich vor KI-gesteuerten. Wir beginnen mit dem Schutz Ihrer E-Mail-Zugangsdaten, anschließend Ihrer Anwendungen und Zugriffe und schützen dann Ihre Daten mit einem sicheren Backup. Für weitere Informationen oder um eine Beratung zu buchen, besuchen Sie unsere Seite zu Ransomware-Lösungen.

Über Barracuda

Barracuda strebt danach, die Welt zu einem sichereren Ort zu machen. Wir glauben, dass jedes Unternehmen Zugang zu Cloud-First-Sicherheitslösungen auf Unternehmensniveau verdient hat, die einfach zu kaufen, zu implementieren und zu verwenden sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die mit unseren Kunden wachsen und sich anpassen. Mehr als 200.000 Organisationen weltweit vertrauen auf den Schutz durch Barracuda – auf eine Art und Weise, von der sie vielleicht nicht einmal wissen, dass sie gefährdet sind. Daher können sie sich darauf konzentrieren, ihr Unternehmen auf die nächste Stufe zu heben. Weitere Informationen dazu unter de.barracuda.com.

Barracuda