KI macht Ransomware noch gefährlicher

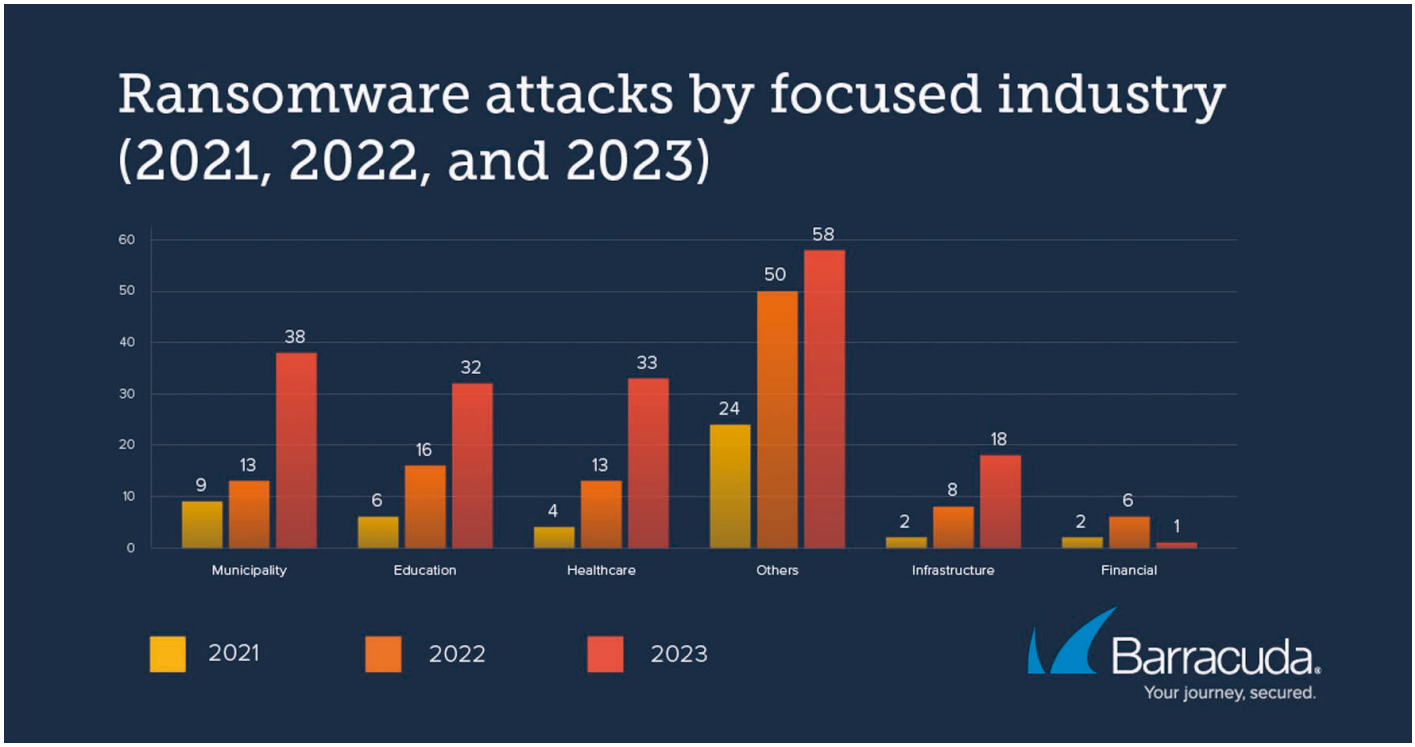

Bild 1: Ransomware-Angriffe haben sich in den letzten Jahren über alle Branchen hinweg vervielfacht.

Autor:
Dr. Klaus Gheri
Vice President & General Manager Network Security
Barracuda Networks
www.barracuda.com

Ransomware ist schon längere Zeit ein echtes Problem für Organisationen jeder Art und Größe. Betrachtet man die neuesten Entwicklungen, ist keine Entwarnung in Sicht. Eher im Gegenteil: Die Kriminellen nutzen mittlerweile KI, um ihre Angriffe noch effizienter zu machen. Die Sicherheitsforscher von Barracuda konnten in einer Untersuchung jüngst belegen, dass sich nicht nur die Quantität von Ransomware-Angriffen sondern auch die Qualität vergrößert hat. Nominal hat sich die Anzahl der gemeldeten Angriffe über alle Branchen hinweg im letzten Jahr verdoppelt - und seit 2021 mehr als vervierfacht. Dies ist zu einem großen Anteil auf KI für Automatisierung zurückzuführen, die den Kriminellen dabei hilft, mehr Angriffe durchführen zu können. Gleichzeitig steigt auch die Qualität. Denn die Angreifer nutzen generative KI um sehr schnell und ohne großen Aufwand gut gestaltete und grammatikalisch korrekte Phishing-E-Mails zu erstellen. KI führt damit dazu, dass man diese E-Mails anhand von Grammatik- und Rechtschreibfehlern kaum noch erkennen kann. Ransomware-as-a-Service-Tools und generative KI für Texterstellung und Codegenerierung machen es Cyberkriminellen mithin immer einfacher, ihrem Handwerk nachzugehen.

Schutz gegen Ransomware ist möglich

Das zeigt die Finanzindustrie. Oberflächlich betrachtet scheint gegen Ransomware kein Kraut gewachsen zu sein. Schaut man sich die Zahlen erfolgreicher Angriffe jedoch nach Industrie an, fällt ein Trend auf: Finanzinstitute werden weniger häufig angegriffen als Öffentliche Verwaltung, Ausbildung oder das Gesundheitswesen. Der Anteil der Ransomware-Angriffe stieg im Jahresvergleich in allen fünf Schwerpunktbranchen - mit Ausnahme von Finanzunternehmen. Angriffe auf Kommunen stiegen von 12 Prozent auf 21 Prozent, Angriffe auf das Gesundheitswesen von 12 Prozent auf 18 Prozent, Angriffe auf das Bildungswesen von 15 Prozent auf 18 Prozent und Angriffe auf die Infrastruktur von 8 Prozent auf 10 Prozent. Im Vergleich dazu gingen die Angriffe auf Finanzinstitute von sechs Prozent auf ein Prozent zurück.

Finanzinstitute sichern sich besser ab

Die Tatsache, dass Finanzinstitute sehr begehrte Opfer mit potenziell hohen Renditen für die kriminellen Angreifer wären, sich diese aber auf die eher klammen Branchen fokussieren, lässt einen klaren Schluss zu: Die Finanzindustrie hat höhere Security-Budgets, ist daher besser abgesichert und die Angreifer müssten deutlich

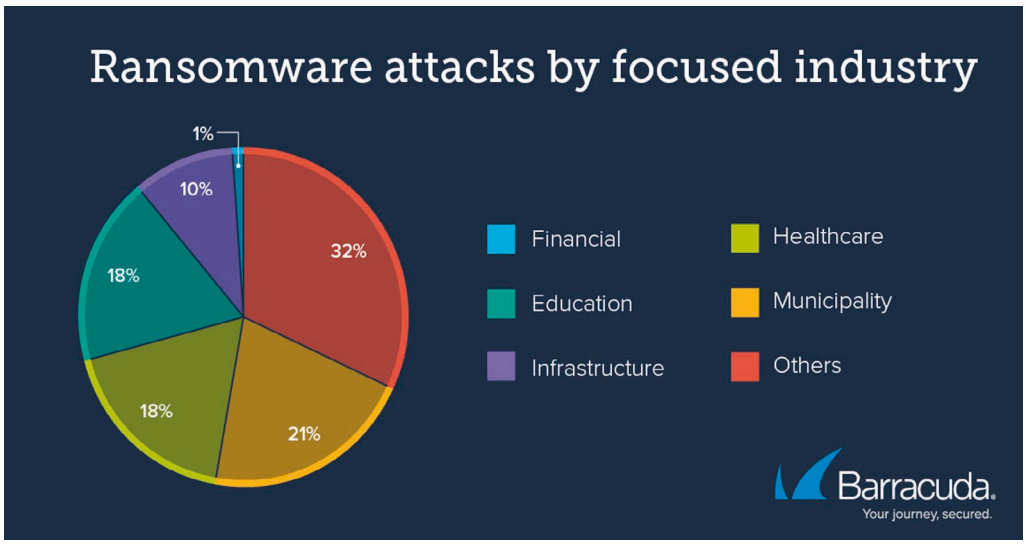

Bild 2: Angreifer fokussieren sich auf weniger geschützte Branchen wie Öffentliche Verwaltung, Ausbildung oder das Gesundheitswesen, die einen höheren ROI versprechen.

mehr in ihre Angriffe investieren. Der zu erwartete Return of Investment ist für die Angreifer daher deutlich niedriger als bei Branchen, die weniger gut abgesichert sind, aber auch weniger Ertrag versprechen. Dank KI werden Ransomware-Angriffe also erfolgreicher und häufiger. Die Finanzindustrie beweist jedoch, dass es möglich ist, sich besser gegen Angriffe zu schützen. Zum einen Teil bedeutet dies für alle anderen Branchen, mehr Ressourcen aufzuwenden, insbesondere wenn die Pläne für Geschäftskontinuitäts- und Notfallwiederherstellung und die genutzten Technologien schon länger nicht mehr aktuell sind. Doch auch jenseits von Neuanschaffungen von Sicherheitstechnologie können Unternehmen einige Maßnahmen umsetzen, um ihre Widerstandsfähigkeit zu verbessern.

Widerstandsfähigkeit verbessern

Fünf Praktiken zur Verbesserung der Widerstandsfähigkeit gegen Ransomware:

1. Erkennung und Prävention
Die Priorität sollte darin bestehen, Maßnahmen und Tools zur Erkennung und Verhinderung eines erfolgreichen Angriffs bereitzustellen. In der heutigen, sich schnell entwickelnden Bedrohungslandschaft bedeutet dies die Implementierung tiefgreifender, mehrschichtiger Sicherheitstechnologien, einschließlich KI-gestütztem E-Mail-Schutz und Zero-Trust-Zugriffsmaßnahmen, Anwendungssicherheit, Bedrohungsjagd, XDR-Funktionen und effektiver Reaktion auf Vorfälle.

2. Widerstandsfähigkeit und Wiederherstellung
Auch mit begrenzten Ressourcen kann man sich effektiv von Ransomware-Angriffen erholen. Zunächst sollte man damit rechnen, dass die Angreifer es auch auf die Infrastruktur für Geschäftskontinuität und Notfallwiederherstellung abgesehen haben - einschließlich der Backup-Systeme. Zahlreiche Vorfälle belegen, dass Angreifer oft erst dann Lösegeld fordern, wenn sie sicher sind, dass das Opfer nur begrenzte Möglichkeiten zur Wiederherstellung hat. Im Folgenden finden sich einige Tipps, wie man sich besser auf Angriffe vorbereitet.

- Sicherungssysteme segmentieren und isolieren
- Einen anderen Speicher für die Benutzerverwaltung verwenden, beispielsweise. ein separates Active Directory und/oder Lightweight Directory Access Protocol
- Stärkere Multifaktor-Authentifizierungsmechanismen (MFA) anstelle von Push-Benachrichtigungen verwenden
- Verschlüsselung verwenden
- Richtlinien und die Dokumentation durch Verschlüsselung und privilegierten Zugriff schützen und in einem anderen Formfaktur aufbewahren

3. Weitere Möglichkeiten zur Sicherung von Backups, Air-Gaps und Cloud-Backups
Das Trennen des Speichers von der typischen Betriebsumgebung des Administrators mittels eines Air-Gaps verbessert dessen Sicherheit. Die Cloud ist in diesem Fall die beste Option. Man muss jedoch bedenken, dass die Wiederherstellung über das Internet etwas langsamer ist als lokale Wiederherstellung. Andere Möglichkeiten zur Verbesserung der Sicherheit von Backups sind:

- Zero Trust für den Zugriff auf eine Backup-Lösung
- Reduzieren des Zugriffs durch rollenbasierte Zugriffskontrolle
- Implementierung von unveränderlichen Dateispeichern
- Vermeidung der „Netzwerkfreigabe“ für die Backup-Umgebung
- Verwendung einer speziell entwickelten, vollständig integrierten Lösung, so dass Software und Hardware zusammengehören

4. Spezielle Backup-Appliances
Hypervisoren für virtuelle Maschinen stellen leider zusätzliche Angriffsflächen dar, die böswillige Akteure nutzen können, um in die Backup-Lösung einzudringen. Daher empfiehlt es sich nach wie vor die Verwendung einer speziellen Backup-Appliance-Lösung, wenn das Ziel der Wiederherstellungszeit (RTO) aggressiv ist. Auf keinen Fall sollten Eigenentwicklungen genutzt werden.

5. SaaS-Anwendungen nicht vergessen
Wichtig ist die Absicherung von Daten, die in der Cloud gespeichert sind. In Microsoft 365-Konten und anderen unter Azure AD registrierten SaaS-Anwendungen liegen wichtige Datenbestände, die eine kontinuierliche Datenklassifizierung, Zugriffskontrolle und Strategie für echten Datenschutz erfordern.

Fazit: Verbesserung der Widerstandsfähigkeit

KI hat Ransomware noch gefährlicher gemacht. Die Angriffe werden dadurch nicht nur besser, sondern auch häufiger. Es gilt also weiterhin, dass Organisationen analog zur Verbesserung von Ransomware, ihre eigene Widerstandsfähigkeit kontinuierlich verbessern müssen, um nicht Opfer zu werden und Lösegeld für die Entschlüsselung von Daten zu bezahlen.

Die Widerstandsfähigkeit gegen Angriffe lässt sich durch zahlreiche Maßnahmen verbessern. Dies beinhaltet neben der Implementierung tiefgreifender, mehrschichtiger Sicherheitstechnologien auch zahlreiche organisatorische Praktiken. ◄