Die Geopolitik hat Einzug in unsere Netze gehalten:

Einblicke in den Cyber Underground

Schwerwiegende Ransomware-Angriffe sorgen täglich für Schlagzeilen. Doch noch eine andere, unsichtbare Bedrohung lauert: Cyber-Wirtschaftsspionage und -Sabotage schaden Unternehmen in Deutschland zunehmend. Es besteht dringender Handlungsbedarf, aber wir sehen, dass Unternehmen oft zögerlich sind. Warum ist das so und wie bekommt man dieses Risiko in den Griff?

von Eileen Walther

Ransomware ist Teil der organisierten Cyberkriminalität, bei der hartgesottene Kriminelle rücksichtslos versuchen, den größten Profit aus Daten, Netzwerken und Unternehmen zu ziehen. Dadurch entstehen der deutschen Wirtschaft jedes Jahr Schäden in Höhe von mehreren hundert Milliarden Euro. Vor mehr als zehn Jahren, als ich noch in der Abteilung für High-Tech-Kriminalität der niederländischen Kriminalpolizei tätig war, haben wir bereits vor dieser sich entwickelnden Bedrohung gewarnt. Ransomware hatte in Russland bereits einen sicheren Hafen, um in diesem Maße aufblühen zu können, da dies seinen geopolitischen Interessen diente.

Es bedurfte allerdings noch vieler verheerender Angriffe, bis europäische Unternehmen das Ausmaß von Ransomware erkannten. Bei Northwave sehen wir mittlerweile, dass unsere Kund:innen sich dessen bewusst sind und unsere Expertise nutzen, um ihre digitale Reise so sicher wie möglich zu gestalten.

Cyberspionage ist auf dem Vormarsch

Unser digitaler Lebensraum hat sich still und leise in eine grenzenlose Kampfzone für internationale Konflikte verwandelt. Unser Computer Emergency Response Team (CERT) kommt weiterhin vor allem bei Ransomware-Angriffen zum Einsatz. Jedoch sind wir zunehmend besorgt über diejenigen Vorfälle, die unentdeckt bleiben. Denn wir stellen fest, dass staatlich gesponserte Advanced Persistent Threats (APTs) extrem zunehmen. Anfang dieses Jahres hat das Bundesamt für Verfassungsschutz (BfV) deutlich gemacht: China ist der Hauptgegner für Deutschland im Bereich der Wirtschafts- und Wissenschaftsspionage. Wir sehen, dass solche Warnungen viele Unternehmen mit der Frage zurücklassen: „Aber warum sollten wir uns darum kümmern. Und selbst wenn, was können wir tun?“

Chinas Cyberstrategie ist weitreichend

Es besteht kein Zweifel: China verfügt über den größten Cyberspionageapparat der Welt, der sich voll und ganz den langfristigen Ambitionen des Landes verschrieben hat. Es strebt aggressiv nach den Technologien, die es braucht, um eine autonome, führende globale Wirtschaftsmacht zu werden. Cyberspionage ist eine Möglichkeit, dies zu erreichen, Übernahmen deutscher Unternehmen eine andere.

Es gibt Dutzende von chinesischen Spionagekampagnen. Die meisten sind seit Jahren aktiv und greifen Netzwerke auf der ganzen Welt an. Jede APT-Gruppe besteht aus bis zu Hunderten von erfahrenen Hackern, Entwicklern und Analysten. Sie dringen in Netzwerke ein und stehlen Informationen in großem Stil: Informationen wie Baupläne, sonstiges geistiges Eigentum oder strategische Informationen deutscher Unternehmen, die die chinesischen Nachrichtendienste direkt an chinesische Unternehmen weitergeben.

Was wir über APT-Gruppen wissen

Es liest sich wie ein Spionage-Thriller, ist aber die bittere Spionage-Wahrheit. Im vergangenen Jahr warnte das BfV vor der Spionagekampagne APT27/Emissary Panda, die es auf deutsche Pharma- und Technologieunternehmen abgesehen hat. Ein weiteres Beispiel ist eine Gruppe namens Mustang Panda, die deutsche Telekommunikationsunternehmen ausspioniert. Unser CERT stößt außerdem in Deutschland regelmäßig auf APT41/Wicked Panda. Neben ihren eigentlichen Spionage-Aktivitäten ist diese Gruppe dafür bekannt, dass sie zusätzlich hin und wieder Ransomware einschleust. Wir haben den Eindruck, dass die Hacker in dem Fall entweder zusätzliches Geld verdienen wollen oder diese Vorgehensweise als Ablenkungsmanöver nutzen.

Die von APT-Gruppen eingesetzten Techniken sind weitaus ausgefeilter und schwieriger zu erkennen als die Ransomware-Methoden, an die wir uns gewöhnt haben. Spear-Phishing ist nach wie vor eine beliebte Methode, die von fast allen APT-Gruppen eingesetzt wird. Darüber hinaus nutzen sie legitime Verwaltungstools und kommerzielle Penetrationstests, um Netzwerke zu infiltrieren.

Foto: Adobe Stock

Eileen Walther,
Country Manager Germany,
Northwave Cyber Security

> Jede APT-Gruppe besteht aus bis zu Hunderten von erfahrenen Hackern, Entwicklern und Analysten.

Was bedeutet das für deutsche Unternehmen?
Industrien wie Telekommunikation, IT, Transport und Logistik, Schifffahrt, Landwirtschaft, Pharmazie,Verteidigung, Energie oder andere Sektoren, in denen innovative Technologien eine wichtige Rolle spielen, sind mit großer Sicherheit strategische Ziele.

Ein Cyberspionage-Angriff kann jahrelang in Netzwerken versteckt sein. In der Zwischenzeit lernen die Angreifer von allem, was Mitarbeitende entwickeln oder produzieren. Der Schaden ist zwar nicht so offensichtlich wie bei einem Ransomware-Angriff, aber er untergräbt Wettbewerbspositionen. Diese Bedrohung trifft Firmen im strategischen Bereich und ist damit Chef:innen-Sache. Geschäftsleitungen sollten Cyberspionage in ihr Risikomanagement einbeziehen.

Was wir Unternehmen raten
Wenn es um angemessenen Schutz geht, betrachten wir APTs als den neuen Maßstab für die Cybersicherheit. Ein umfassendes Sicherheitsmanagement ist unerlässlich, denn APTs haben Zeit. Mitarbeitende, IT-Anbieter und Lieferanten sind nützliche Trittbretter. Das Zusammenspiel von adäquaten organisatorischen, menschlichen und technischen Maßnahmen wird zunehmend wichtig. APT-Angriffe sind für ein SOC (Security Operations Center) schwieriger zu erkennen. Man kann sich nicht nur auf KI-unterstützte Erkennungstools verlassen. Für adäquates Monitoring braucht man hochqualifizierte Security-Analyst:innen und -Spezialist:innen.

Die Geopolitik mag heimlich in unsere Netze eingedrungen sein. Aber im Gegensatz zu den internationalen politischen und militärischen Konflikten haben Unternehmen die Kontrolle über ihr eigenes Netzwerk und die Möglichkeit, die Risiken in den Griff zu bekommen. ■

northwave-cybersecurity.com/de

Advertorial

Daten da schützen, wo sie sich befinden

Unternehmensdatenschutz in einer hybriden, Cloud-basierten und KI-gestützten Welt

von Thomas Wethmar

Die Bedrohungslage in der Cybersecurity ist brisant: Die Zahl der Angriffe nimmt stetig zu und auch die Kosten, die mit einer Attacke einhergehen, steigen weiter. Der Grund dieser Eskalation ist, dass sich die Art, wie wir arbeiten, radikal verändert hat: An die Stelle der zentralisierten Netzwerke von früher treten immer öfter dezentrale Infrastrukturen mit Tausenden von Endpunkten und Apps – häufig mit einer brandgefährlichen Schatten-IT, in der niemand mehr weiß, wer welche Applikationen benutzt und wo sich welche Daten befinden. Datenverluste sind an der Tagesordnung, auch aufgrund von KI-Tools wie ChatGPT, in denen heute etliche Gigabyte sensibler Daten hochgeladen werden, ohne groß über die Security- und Compliance-Folgen nachzudenken.

Security-Awareness wächst
Die gute Nachricht ist, dass das Bewusstsein für diese Gefahren zunimmt und die Security-Verantwortlichen durchaus gewillt sind, in Lösungen wie Data Leak Prevention und Zero Trust zu investieren. Wenn die Investments die gewünschte Wirkung zeigen sollen, müssen die Unternehmen bei der Implementierung allerdings drei Aspekte im Blick behalten:

- **Granulare Visibilität:** Unternehmen müssen einen detaillierten Überblick über die Tools erhalten, die ihre Mitarbeitenden verwenden, und das Risikopotenzial jeder Anwendung bewerten.
- **Monitoring & Kontrolle:** Dann gilt es zu entscheiden, welche Apps gestattet werden und welche Daten Anwender übermitteln dürfen. Diese Regeln werden über granulare Policies durchgesetzt und kontinuierlich überwacht.
- **Data Leak Prevention:** Dedizierte DLP-Lösungen können ergänzend Datenverluste in Cloud- und AI-Apps verhindern, etwa indem sie die Konversationshistorie deaktivieren und Uploads der Benutzer limitieren. Flankierend sollten Mitarbeitende in der Nutzung generativer AI-Tools geschult werden.

Grundsätzlich gilt: Wer Daten in der Cloud schützen will, muss selbst Teil der Cloud werden. Denn nur Cloud-native Plattformen bieten die Transparenz, Skalierbarkeit und Resilienz, die nötig ist, um die enormen Datenmengen von heute unter Kontrolle zu behalten. Umgekehrt heißt dies aber auch: Wenn es uns mit zeitgemäßen, hybriden Plattformen gelingt, Daten On-Premises und ebenso in der Cloud zu schützen und das volle Potenzial der Cloud zu erschließen, können wir neben gespeicherten Daten auch diejenigen Daten abdecken, die gerade verarbeitet werden – wir erreichen also einen wesentlich besseren Schutz der Unternehmensdaten und heben das Schutzniveau auf das nächste Level. ■

Thomas Wethmar,
Regional Director DACH,
Skyhigh Security

> Wer Daten in der Cloud schützen will, muss selbst Teil der Cloud werden.

skyhighsecurity.com

Foto: AdobeStock