Schutzlücken bei Europas KMU: Ransomware-Angriffe seit Jahresbeginn verdoppelt

Franziska Geier, Geschäftsführerin von Stoïk Deutschland © Stoïk

Innerhalb der ersten Monate des Jahres hat sich die Anzahl der Ransomware-Attacken auf Unternehmen in Europa mehr als verdoppelt. Diese Zahl veröffentlicht Stoïk, führender Anbieter von Cyberversicherungen für Gewerbe- und Industrieunternehmen mit über 6.000 versicherten Unternehmen in Deutschland, Frankreich, Spanien und Österreich, anlässlich des internationalen Ransomware-Aktionstages am 12. Mai 2025. Stoïk möchte damit auf die stark zunehmende Bedrohung durch Ransomware aufmerksam machen.

Ransomware im Wandel: Verdopplung der Angriffe und schwerwiegende Folgen

Laut aktuellen Daten stieg die Frequenz der Ransomware-Fälle bei Stoïk-Kunden von 0,54 Prozent im Jahr 2024 auf 1,1 Prozent in den ersten Monaten von 2025: “Ransomware-Angriffe stellen für mittelständische Unternehmen eine existenzielle Gefahr dar, weil sie nicht nur Betriebsunterbrechungen und finanzielle Verluste verursachen, sondern vor allem Geschäftsbeziehungen gefährden. Häufig trennen Partner vorsorglich sämtliche digitalen Verbindungen, um eigene Risiken zu minimieren. Das betroffene Unternehmen muss anschließend mit hohem Aufwand Sicherheitsnachweise erbringen und Vertrauen mühsam wiederherstellen – oft noch Tage oder Wochen, nachdem die IT-Systeme bereits wieder sicher sind. Ein einziger Angriff kann somit langfristige Vertrauensverluste bedeuten“, sagt Vincent Nguyen, Leiter Cybersicherheit bei Stoïk.

Ebenfalls kommt die sogenannte „Triple Extortion“ häufiger vor, bei der Täter nicht nur Unternehmensdaten verschlüsseln, sondern zusätzlich Kunden und Partner mit Veröffentlichung gestohlener Daten bedrohen, um höhere Lösegelder zu erzwingen. Insgesamt hat sich die Zeitspanne zwischen der Entdeckung einer Schwachstelle und ihrer Ausnutzung dramatisch verkürzt, was eine erhöhte Wachsamkeit und bessere Reaktionsmöglichkeiten von Unternehmen verlangt.

Angreifer haben es leichter - osteuropäische Cybercrime-Gruppen nehmen zu

Das größte Risiko besteht heute nicht so sehr in der Nutzung künstlicher Intelligenz zur automatisierten Suche nach Schwachstellen, sondern in der Leichtigkeit, mit der Cyberkriminelle an Zugangsdaten gelangen. Vor allem sogenannte Infostealer treiben diese Entwicklung voran: Diese unauffälligen Schadprogramme sammeln auf kompromittierten Rechnern gezielt sensible Daten wie Passwörter, Zertifikate und Authentifizierungsinformationen – und öffnen Angreifern damit Tür und Tor zu Unternehmensnetzwerken.

Als eine weitere Ursache für den Anstieg der Angriffe sehen die Cybersicherheitsexperten von Stoïk vor allem das Wiedererstarken osteuropäischer Cybercrime-Gruppen und das Geschäftsmodell „Ransomware as a Service“ (RaaS) welches sich auf dem Vormarsch befindet, das auch technisch weniger versierten Kriminellen ermöglicht, komplexe Angriffe durchzuführen.

Zu viele Schwachstellen: Unternehmen hätten Angriffe vermeiden können

Die Beobachtungen von Stoïk zeigen, dass die meisten Vorfälle auf menschliches Versagen oder bekannte, nicht behobene Schwachstellen zurückzuführen sind: “Zu viele Unternehmen werden immer noch von Angriffen überrascht, die eigentlich vermeidbar wären. Durch die Aktivierung der Multi-Faktor-Authentifizierung (MFA), d. h. das Auferlegen einer zusätzlichen Validierung für den Zugriff auf sensible Systeme, kann ein Großteil der Angriffe durch Passwortdiebstahl abgewehrt werden”, so Nguyen.

Auf Basis seiner umfassenden Erfahrung empfiehlt Stoïk Unternehmen drei konkrete Maßnahmen, um sich wirksam gegen die zunehmende Bedrohung durch Ransomware-Angriffe zu schützen.

- Einführung der Multi-Faktor-Authentifizierung (MFA) für sämtliche externe Zugriffe, insbesondere VPN-Verbindungen.
- Aktive Überwachung und schnelle Behebung bekannter Sicherheitslücken gemäß den Anforderungen der neuen EU-Richtlinie NIS-2.
- Regelmäßige, vom Hauptnetzwerk getrennte Back-ups der Unternehmensdaten.

So schützt Stoïk seine Kunden vor Cyberangriffen:

Um Unternehmen besser vor diesen Cyberbedrohungen zu schützen, hat Stoïk das Sicherheits-Tool „Stoïk Protect“ verbessert, das jetzt auch kompromittierte Benutzerkonten mittels Infostealer-Analyse frühzeitig erkennt. Zudem bietet das Managed Detection and Response (MDR)-Angebot von Stoïk effektiven Schutz: „Bislang erlitt keines der durch Stoïk MDR geschützten Unternehmen eine Ransomware-Attacke“, erläutert Nguyen.

Stoïk versteht Cyberversicherung nicht nur als reine Schadensregulierung, sondern als integralen Bestandteil einer proaktiven Sicherheitsstrategie. Durch eine Kombination aus Prävention, Frühwarnsystemen und schneller Reaktion unterstützt Stoïk mittelständische Unternehmen, ihre Widerstandsfähigkeit gegen Cyberangriffe nachhaltig zu stärken.

Stoïk Protect und Stoïk MDR bieten effektiven Schutz gegen Ransomware

1. Stoïk Protect – Umfassendes Cyber-Monitoring

- Erweiterter externer Sicherheitsscan:

Stoïk Protect führt kontinuierliche Analysen der extern sichtbaren IT-Systeme von Kundenunternehmen durch und identifiziert dabei Schwachstellen und fehlerhafte Konfigurationen frühzeitig. Neu ist die gezielte Auswertung sogenannter „Infostealer-Logs“, um kompromittierte Nutzerkonten zu erkennen, bevor Angreifer diese missbrauchen können.

- Frühwarnsystem für Angriffe:

Durch systematische Überwachung potenzieller Einfallstore erhält das Stoïk CERT-Team frühzeitig Warnungen, sodass es Unternehmen proaktiv und individuell über konkrete Sicherheitsrisiken informieren und bei deren Beseitigung unterstützen kann.

2. Stoïk MDR – Managed Detection and Response

- Aktiver Schutz der Endpunkte:

Stoïk MDR überwacht permanent die Endgeräte und Server der versicherten Unternehmen auf verdächtige Aktivitäten und potentielle Anzeichen für Cyberangriffe. Verdachtsfälle werden durch das CERT-Team rund um die Uhr analysiert und abgewehrt.

- Mehr Schutzwirkung gegen Ransomware:

Seit Einführung von Stoïk MDR verzeichnet Stoïk keinen einzigen erfolgreichen Ransomware-Vorfall bei Kunden, die diesen Dienst nutzen. Dies zeigt eindrucksvoll, wie entscheidend frühzeitige Erkennung und unmittelbare Reaktionsfähigkeit für die Verhinderung von Schäden sind.