

# INPUT

Das Fachmagazin der Neo One AG

## DIE ALLTAGSREALITÄT

Wie digitale Chancen und Risiken die Wirtschaft,  
Gesellschaft und Geopolitik prägen.

## Liebe Kund:innen, Partner:innen und Freund:innen von Neo One

Sie halten die erste Ausgabe von «INPUT» in Ihren Händen. Mit diesem regelmässig erscheinenden Magazin geht Neo One einen neuen Weg: Unser Anspruch ist es, relevante Themen rund um ICT, Cybersicherheit und Unternehmensführung aus unterschiedlichen Perspektiven zu beleuchten – verständlich, praxisnah und inspirierend. Wir möchten damit nicht nur informieren, sondern auch Orientierung in einer zunehmend digitalen Welt geben, Denkanstösse liefern und konkrete Tipps für Führungskräfte und IT-Verantwortliche bereitstellen. Mit «INPUT» teilen wir unser Wissen, ordnen Entwicklungen ein und schaffen echten Mehrwert für unsere Kunden, Partner und alle anderen, die sich für IT interessieren – ganz nach unserem Motto: Persönlich. Fundiert. Ganzheitlich.

Die erste Ausgabe von «INPUT» dreht sich rund um das drängende Thema Ransomware – eine Bedrohung, die mittlerweile alle Unternehmen betrifft. Denn Ransomware (Erpressungssoftware; von Englisch ransom für «Lösegeld») im Jahr 2025 ist mehr als ein IT-Security-Problem. Ransomware ist ein Risiko, das Unternehmen, Verwaltungen und Organisationen permanent herausfordert. 44 Prozent aller Cybervorfälle gehen heute laut dem Arctic Wolf Threat Report auf Ransomware zurück. Auf den jährlich erscheinenden Bericht des renommierten Cybersecurity-Unternehmens zählen weltweit zahlreiche Unternehmen und Organisationen. Und obwohl Strafverfolger grosse Gruppen wie LockBit oder BlackCat zerschlagen haben, ist die Bedrohung nicht kleiner geworden – im Gegenteil: Kleinere, agile Banden haben das Vakuum gefüllt und agieren mittels neuer Tools, künstlicher Intelligenz und raffinierter Tricks noch umfassender und unberechenbarer.

Diese Professionalisierung von Cybercrime hat gravierende Folgen für Unternehmen. Für sie stellt sich nicht mehr die Frage, ob sie einem Cyberangriff zum Opfer fallen, sondern wann – und wie sie sich darauf vorbereiten. Moderne Backup-Strategien allein greifen zur Prävention nicht mehr.

Gefragt sind etwa Zero-Trust-Architekturen, KI-gestützte Erkennungssysteme oder Incident-Response-Playbooks. Doch klafft eine Lücke zwischen Theorie und Umsetzung: Nur die Hälfte der Unternehmen kann ihre Notfallpläne im Ernstfall tatsächlich effektiv umsetzen. Die Folgen sind gravierend: Neben hohen Lösegeldforderungen verursachen vor allem der Reputationsverlust und Betriebsunterbrüche langfristige Schäden. Besonders im Fokus der Cyberkriminellen stehen KMU, die weder die personellen noch die finanziellen Ressourcen haben, um hochprofessionellen Angreifern Paroli zu bieten. Für uns bei Neo One steht fest: Ransomware ist für Unternehmen eine der gefährlichsten Bedrohungen unserer Zeit. Sie zwingt Organisationen, Cybersicherheit nicht als technische Disziplin zu begreifen, sondern als Kernaufgabe von Management und Fachabteilungen – sowie des gesamten Personals, das zwingend auf aktuelle Bedrohungen sensibilisiert werden muss.

Eine interessante Lektüre und weiterhin viel Erfolg wünscht  
Jan Braunschweiler, CEO,  
Inhaber und Verwaltungsratspräsident der Neo One AG



# INHALT

4

Mythen & Fakten



Es gibt viele Irrtümer um das Thema Ransomware. Wir räumen auf mit falschen Annahmen.

6

Schwerpunkt



Was ist Ransomware und wie hat sich die Methode entwickelt? Die Hintergründe zum Thema.

14

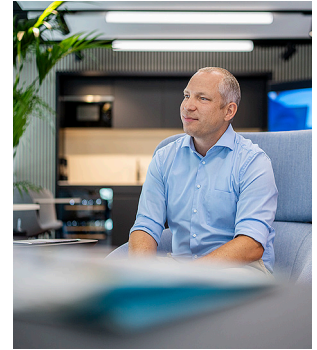
Interview



Was passiert bei einem Angriff? Der CEO eines geschädigten Unternehmens erzählt.

20

Standpunkt



Nützt im Ernstfall eine Cyberversicherung? Ein Experte erklärt, warum sich ein solcher Schutz lohnt.

24

Erfolgsgeschichte | Partnerschaft mit Weitblick.

27

Fachchinesisch | Die wichtigsten Begriffe rund um Ransomware.

28

Wegweiser | Was tun, wenns passiert?

30

Der Experte erzählt | Offene Türen für Angreifer.

32

Trendradar | Verteidigung und Angriff: Das ständige Wettrüsten.

34

Lösungen | Wie Neo One gezielt vor Ransomware schützt.

---

## «Ransomware bleibt eine der bedeutendsten Cyberbedrohungen für Unternehmen aller Branchen und Grössen.»

---

Max Klaus, Stellvertretender Medien- und Informationsverantwortlicher beim Bundesamt für Cybersicherheit (BACS), auf Seite 19.

### Impressum:

Herausgeberin:  
Neo One AG, Grindelstrasse 6, 8303 Bassersdorf  
E-Mail: [hello@neo-one.ch](mailto:hello@neo-one.ch), [www.neo-one.ch](http://www.neo-one.ch)  
Standort Luzern, Schnydermatt 1, 6210 Sursee



# SECHS IRRTÜMER RUND UM RANSOMWARE

Weil das Thema Ransomware technisch komplex ist und betroffene Unternehmen aus Angst vor Reputationsschaden nicht gerne über konkrete Vorfälle berichten, kursieren viele Halbwahrheiten und falsche Annahmen rund um das Thema Ransomware. Zudem verlassen sich Entscheider ohne IT-Hintergrund oft auf vereinfachte Erklärungen, was zu falschen Vorstellungen über Angriffe, deren Folgen und Schutzmassnahmen führt.

1

## «Ein Backup schützt zuverlässig vor negativen Folgen eines Ransomware-Angriffs.»

Zwar sind Backups elementar und ein zentraler Bestandteil jeder Sicherheitsstrategie – doch kein Garant dafür, dass ein Unternehmen bei einem Ransomware-Angriff keinen Schaden nimmt. Backups sind nur dann wirksam, wenn sie korrekt verwaltet und regelmässig getestet werden. In der Praxis zeigt sich oft, dass zwar Backups existieren, diese aber entweder im gleichen Netzwerk gespeichert sind und daher ebenfalls verschlüsselt wurden, nicht aktuell sind oder seit Monaten nicht mehr auf ihre Wiederherstellbarkeit geprüft wurden. Sichere Backups müssen regelmässig erstellt und vom produktiven Netzwerk getrennt werden – etwa offline oder in der Cloud.

2

## «Nur grosse Unternehmen sind betroffen.»

Ransomware macht keinen Unterschied zwischen KMU und Grosskonzernen. Im Gegenteil: Kleine und mittlere Unternehmen stellen oft ein leichtes Ziel dar, da sie häufig über weniger strukturierte IT-Sicherheitsmassnahmen verfügen. Für viele Angreifer sind KMU lukrative «low hanging fruits»: leicht zu kompromittieren, aber dennoch mit sensiblen Daten und entsprechend hohem Druck zur Wiederherstellung der Systeme. Eine Antivirensoftware, ein Backup oder eine Firewall vermitteln oft ein trügerisches Gefühl der Sicherheit. Zudem denken viele Geschäftsleiter kleiner Firmen, dass sie für Cyberkriminelle schlicht uninteressant sind. Diese Haltung ist weitverbreitet – und gefährlich. Die meisten Ransomware-Kampagnen funktionieren nicht über gezielte Auswahl, sondern durch massenhaftes Scan-

ning nach Schwachstellen, durch automatisierte E-Mails oder die Ausnutzung weitverbreiteter Sicherheitslücken. KMU geraten dabei genauso ins Visier wie grössere Organisationen. Oft sind es gerade kleinere Betriebe, die schneller zahlungsbereit sind – was sie zu attraktiven Zielen macht.

3

## «Wenn ich Lösegeld bezahle, bekomme ich meine Daten zurück.»

Es gibt keine Garantie, dass die Angreifer nach Zahlung des Lösegelds tatsächlich einen funktionierenden Entschlüsselungscode liefern, mit dem die Daten sicher und vollständig wiederhergestellt werden können. Zudem erhöht man mit einer Lösegeldzahlung das Risiko, bei künftigen Angriffen erneut ins Visier zu geraten: Wer bezahlt, signalisiert Zahlungsbereitschaft und landet oft auf einschlägigen Listen («Repeat Victim Targeting»). Behörden, Security-Experten und Cyberversicherer raten explizit von solchen Lösegeldzahlungen ab.

4

## «Cybersecurity ist Sache der IT-Abteilung.»

Technische Schutzmassnahmen sind wichtig, aber sie greifen nur, wenn das ganze Unternehmen eingebunden ist. Ein häufiges Einfallstor für Ransomware ist menschliches Fehlverhalten – etwa, wenn Mitarbeitende einen infizierten E-Mail-Anhang öffnen oder schwache Passwörter verwenden. Eine verbindliche Sicherheitskultur muss deshalb im ganzen Unternehmen verankert werden, etwa durch regelmässige Schulungen, klare Richtlinien und ein Bewusstsein dafür, dass Cybersicherheit eine gemeinsame Aufgabe ist.