Südtiroler
Wirtschaftszeitung
Wochenblatt für Wirtschaft und Politik

Tiratura: 4.500
Data: 17/04/2026 | **Pagina:** 5
Categoria: Waren- und Dienstleistungsgenossenschaften Print & Web

Cyberangriffe auf Rekordkurs

CYBERKRIMINALITÄT – Täuschend echt, hochprofessionell und längst Teil unseres Alltags: Cyberangriffe nehmen rasant zu. **Wie Hacker heute vorgehen, warum niemand sicher ist – und was Unternehmen jetzt wissen müssen.**

Foto: Shutterstock/PeopleImages

Bozen – Werbung im Radio, in Zeitungen und auf Internetseiten, Warnhinweise in Apps, Sicherheitstipps auf Plakatwänden: Cybersecurity ist plötzlich allgegenwärtig. Doch handelt es sich dabei nur um einen neuen Marketingtrend – oder wächst die digitale Bedrohung tatsächlich? Die Antwort ist eindeutig: kein Trend, sondern Realität. Die Gefahr ist größer geworden – und zwar massiv.

Ein aktueller Vorfall zeigt, wie allgegenwärtig die Gefahr auch in Südtirol ist: Im Zuge eines Hackerangriffs auf den IT-Dienstleister des Hoteliers- und Gastwirteverbandes (HGV), Yanovis, wurden 3.000 gefälschte E-Mails an Urlaubsgäste verschickt. Darin wurden die Empfänger aufgefordert, rasch zu überweisen, da sonst ihre Buchungen storniert würden. Glücklicherweise gelang es den Angreifern laut dem HGV nicht, auf Kreditkartendaten zuzugreifen.

Zahlen, die alarmieren

Was lokal geschieht, ist Teil eines globalen Trends. Cyberkriminalität hat weltweit deutlich zugenommen – und sie trifft längst nicht mehr nur Großkonzerne, sondern auch kleine Betriebe, öffentliche Institutionen und Privatpersonen. Das Internet Crime Complaint Center (IC3) des FBI meldete für das Jahr 2025 mehr als eine Million Beschwerden sowie Schäden in Höhe von rund 20,9 Milliarden US-Dollar. Auch wenn sich diese Zahlen überwiegend auf die Vereinigten Staaten beziehen, gelten sie als verlässlicher Gradmesser für globale Entwicklungen, da Cyberkriminalität längst grenzüberschreitend organisiert ist.

Auch in Italien zeigt sich dieser Trend klar. Die nationale Cyberagentur ACN registrierte allein im ersten Halbjahr 2025 rund 1.500 Cyber-Angriffe – ein Anstieg von 53 Prozent gegenüber dem Vorjahreszeitraum. Gleichzeitig bearbeitete die Postpolizei über 51.500 Fälle von Internetkriminalität, darunter mehr als 27.000 wirtschafts- und finanzbezogene Cyberbetrugsdelikte. Der entstandene Schaden belief sich auf mehr als 269 Millionen Euro.

> Cyberkriminalität ist heute ein hochgradig arbeitsteiliges Geschäftsmodell.
>
> Stefan Laimer

Gleichzeitig werden die Angriffe immer ausgefeilter und professioneller. Cyberkriminalität ist längst kein Randphänomen mehr, sondern eine der zentralen Herausforderungen der digitalen Gegenwart.

Die neue Logik der Täter

Für Stefan Laimer, Head of Security Operations beim IT-Dienstleistungsunternehmen Konverto, ist klar: „Die mediale Aufmerksamkeit ist berechtigt."

Foto: Konverto

Stefan Laimer

Cyberkriminalität sei heute ein hochgradig arbeitsteiliges Geschäftsmodell. Professionelle Gruppen agierten wie moderne Unternehmen: Die einen entwickeln Schadsoftware, die anderen spähen Schwachstellen aus, wieder andere übernehmen Erpressung und Vermarktung gestohlener Daten.

Diese Professionalisierung sei einer der Gründe, warum die Zahl der Vorfälle steige. Der andere: Angriffe seien einfacher geworden. Künstliche Intelligenz habe die Hürden gesenkt, die Qualität erhöht und das Tempo beschleunigt, so Laimer. Auch Hannes Lösch, CEO des IT-Unternehmens Limendo, beobachtet diese Zuspitzung. „Cyberangriffe haben massiv zugenommen", sagt er. Vor allem mit dem Aufstieg von KI und Sprachmodellen sei es für Betrüger viel leichter geworden, glaubwürdige Attacken zu starten.

Der Angriff beginnt beim Menschen

Wer an Cyberangriffe denkt, hat oft Hacker in dunklen Kellern, komplizierte Codes und Hightech-Attacken vor Augen. In der Realität beginnt der Angriff heute aber oft viel banaler: mit einer Mail, einer SMS oder einer WhatsApp-Nachricht. „Diese Attacken starten zu über 90 Prozent beim Menschen", sagt Lösch. „Genau dort setzen Täter an – nicht, weil Technik unwichtig wäre, sondern weil Vertrauen oft leichter zu knacken ist als ein Sicherheitssystem."

Hannes Lösch

Weltweit stechen derzeit drei Angriffsmuster besonders hervor: Phishing und Identitätsdiebstahl, das Ausnutzen von Schwachstellen in öffentlich erreichbaren Systemen und Angriffe über Dritte oder Lieferketten. Gleichzeitig bleibt Ransomware – eine Schadsoftware, die Daten verschlüsselt oder Systeme sperrt, um Lösegeld zu erpressen – eine der gefährlichsten Waffen digitaler Erpresser.

Besonders brisant: Die Methoden haben sich weiterentwickelt. Aus der klassischen Verschlüsselung von Daten sei vielfach eine doppelte Erpressung geworden: „Daten werden erst gestohlen und dann verschlüsselt", sagt Stefan Laimer. Der Druck auf Unternehmen steige damit enorm, weil nicht nur der Betrieb stillsteht, sondern auch die Veröffentlichung sensibler Informationen droht. Und Lösch fügt hinzu: „Mittlerweile soll man nicht mehr dafür zahlen, dass man seine Daten zurückbekommt, sondern dafür, dass sie nicht veröffentlicht werden."

Südtirol: Eng vernetzt, schnell verwundbar

Gerade in Südtirol bekommt die Bedrohungslage eine besondere Dynamik. Die Wirtschaftsstruktur ist kleinteilig, viele Betriebe arbeiten eng zusammen, man kennt sich, vertraut einander und ist digital oft direkt mit Partnern, Dienstleistern oder Kunden verbunden. Genau das macht Angriffe besonders heikel.

Denn Cyberkriminelle zielen laut Stefan Laimer nicht nur auf große Konzerne, sondern gerade auch auf Unternehmen, die sich über alltägliche Abläufe und bekannte Kontakte täuschen lassen. „Besonders in Südtirols eng vernetzter Wirtschaft ist das gefährlich", sagt er. Kriminelle imitierten bekannte Partner oder Vorgesetzte heute so geschickt, dass sie Sicherheitsbarrieren über menschliches Vertrauen umgingen. Dazu kommt: Viele Angriffe seien opportunistisch. Ein Unternehmen werde also genau dann zum Ziel, wenn es durch mangelnde Absicherung seine Verwundbarkeit signalisiere.

Entscheidend sei deshalb nicht nur die eigene IT-Sicherheit, sondern auch, wie gut externe Schnittstellen, Fernzugänge und digitale Partner abgesichert sind. In einem Raum wie Südtirol, wo die Wege kurz und die Netzwerke dicht seien, könne genau diese Nähe zum Risiko werden, so Laimer.

Alte Systeme, neue Risiken

„Viele Unternehmen, die vor 30 Jahren gegründet wurden, sind heute in Bedrängnis, weil sie in alten Technologien stecken", so Hannes Lösch. Veraltete Strukturen vergrößerten die Angriffsfläche erheblich.

Laimer beschreibt, wie solche Schwachstellen heute ausgenutzt werden: Angreifer scannten das Internet automatisiert nach offenen Zugängen, veralteten Webservern oder schlecht abgesicherten Fernwartungssystemen. „Sobald eine technische Lücke oder ein menschlicher Fehler identifiziert ist, erfolgt der Zugriff oft innerhalb von Minuten", sagt er. Danach bewegten sich die Täter häufig zunächst unauffällig weiter im System, bis sie genügend Zugriffsrechte gesammelt hätten, um den eigentlichen Schlag auszuführen.

Vor diesem Hintergrund stellt sich für viele Unternehmen eine grundlegende Frage: Wie sicher ist die eigene Infrastruktur – und wo sollte sie betrieben werden?

Cloud oder eigener Server?

Eine weitere Schwachstelle in der Praxis seien lokale Server, so Hannes Lösch: „Ein lokaler Server ist für mich klar gefährlicher als ein Cloud-Produkt." Der Grund: Während viele Unternehmen ihre eigene Infrastruktur nur mit kleinen Teams oder Externen betreuen,

> Die Attacken starten zu über 90 Prozent beim Menschen.
>
> Hannes Lösch

stünden hinter großen Cloud-Anbietern internationale Sicherheitsteams mit enormen Ressourcen. „Wir bei Limendo haben keinen eigenen Server, weil ich sage: Wir könnten ihn nicht gut schützen."

Stefan Laimer von Konverto setzt hier auf das sogenannte Zwiebelprinzip – ein mehrschichtiges Sicherheitskonzept aus Multi-Faktor-Authentifizierung, regelmäßigen Updates, Backup-Strategien, Netzsegmentierung und einem klaren Incident-Response-Plan. Für ihn ist entscheidend, dass Sicherheit nicht aus einer einzelnen Maßnahme besteht, sondern aus vielen sauber ineinandergreifenden Ebenen.

Doch selbst die beste Infrastruktur ist nur so sicher wie ihre Endgeräte. Besonders Smartphones rücken deshalb zunehmend in den Fokus.

Private Smartphones, geschäftliche Risiken

Smartphones sind aus dem Arbeitsalltag nicht mehr wegzudenken. Doch genau darin liegt eine wachsende Gefahr für Unternehmen. Ein kompromittiertes Gerät kann direkten Zugriff auf geschäftliche E-Mails, Online-Dienste und sensible Unternehmensdaten ermöglichen. Besonders kritisch wird es, wenn über private Smartphones auf Firmenressourcen oder persönliche Cloud-Speicher zugegriffen wird, in denen geschäftliche Zugangsdaten gespeichert sind.

Cybercrime-Experte Laimer warnt vor dieser Gefahr. Um das Risiko zu minimieren, empfiehlt er den Einsatz verwalteter Firmengeräte: „Durch Mobile-Device-Management-Lösungen lassen sich Sicherheitsupdates, Konfigurationen und Verschlüsselungen zentral durchsetzen." Sein Rat für den Alltag: Apps ausschließlich aus offiziellen Stores laden, Berechtigungen restriktiv vergeben und SMS-Links konsequent ignorieren.

Besonders heikel ist die Entwicklung im mobilen Finanzbereich. Online-Banking auf dem Smartphone ist längst Alltag – und damit ein attraktives Ziel für Cyberkriminelle. Vor allem Android-Geräte geraten stärker in den Fokus, weil Banking-Trojaner dort versuchen, Apps zu überwachen, Einmalcodes abzugreifen oder sogar unbemerkt Transaktionen zu autorisieren. „Das größte Risiko besteht in spezieller Malware, die sich als harmlose App tarnt und darauf ausgelegt ist, Zugangsdaten von Banking-Apps zu stehlen", so Stefan Laimer.

Bei Apple-Geräten gilt dieses Risiko als geringer. „iPhones sind sicherer, weil sie in einem geschlossenen Ökosystem betrieben werden und Apps vor der Veröffentlichung streng geprüft werden", erklärt Hannes Lösch. Dennoch bleibe entscheidend, dass Nutzer Sicherheitsupdates installieren und umsichtig mit ihren Daten umgehen.

Die wichtigste Verteidigung bleibt menschlich

Bei aller Technik rückt am Ende der Mensch in den Mittelpunkt – nicht nur als potenzielle Schwachstelle, sondern auch als wichtigste Verteidigung.

„Menschen schulen – das ist Priorität Nummer eins", sagt Lösch. Wer verdächtige Nachrichten erkennt, im Zweifel nachfragt und nicht unter Druck reagiert, könne viele Angriffe bereits im Ansatz stoppen – im privaten wie im beruflichen Umfeld.

Auch Stefan Laimer betont die zentrale Rolle der Mitarbeitenden: Sie seien häufig das erste Ziel, könnten aber zugleich zur stärksten Verteidigungslinie werden. Entscheidend sei eine gelebte Sicherheitskultur, in der Verdachtsmomente ernst genommen und Fehler offen gemeldet werden. Nicht Perfektion schütze ein Unternehmen, sondern Reaktionsfähigkeit.

Wohin die Reise geht

Ein Blick nach vorn zeigt: Die Bedrohung entwickelt sich rasant weiter – und die Aussichten sind alles andere als beruhigend. Mehr KI-gestütztes Social Engineering, mehr Deepfakes, mehr Identitätsmissbrauch sowie verstärkte Angriffe auf mobile Geräte und Lieferketten: Die Gefahr werde in den kommenden Jahren nicht verschwinden, sondern präziser, schneller und glaubwürdiger werden. Darin sind sich Stefan Laimer und Hannes Lösch einig.

Für die beiden Experten steht fest: Cyberkriminalität ist heute ein professionelles Geschäftsmodell, das immer effizienter wird. Und sie beginnt oft nicht mit einem spektakulären Hack, sondern mit einem einzigen falschen Klick.

Antonia Sell
antonia@swz.it