

Foto: Adobe Stock

Volle Attacke

CYBERSICHERHEIT – Hackerangriffe haben letzthin auch Südtirol erschreckt. **Zu glauben, das eigene Unternehmen sei zu unbedeutend für die Kriminellen, wäre ein grober Fehler.** Wo im KI-Zeitalter die Risiken lauern und wie sich Unternehmen schützen können.

BOZEN – Zuletzt hatten Cyberattacken auch in Südtirol für Aufsehen gesorgt: mehrere Unternehmen, darunter industrielle Betriebe wie Intercable, mussten einen Produktionsstopp hinnehmen und waren tagelang nur eingeschränkt arbeitsfähig. Solche Vorfälle zeigen: Die Bedrohung ist real, betrifft längst nicht mehr nur große Konzerne und kann jedes Unternehmen treffen – unabhängig von Größe, Branche oder Standort. Angesichts der wachsenden Komplexität und Professionalisierung moderner Cyberkriminalität gewinnt daher ein proaktiver und vorausschauender Ansatz in der IT-Sicherheit an Bedeutung. Die digitale Transformation bringt enorme Vorteile, gleichzeitig erhöht sie auch die Angriffsfläche: vernetzte Systeme, Cloud-Dienste, mobile Arbeitsformen und der Einsatz von Künstlicher Intelligenz (KI) eröffnen Cyberkriminellen immer neue Einfallstore. Hinzu kommt, dass Angriffe heute gezielter, schneller und schwerer zu erkennen sind – oft nutzen sie menschliche Schwachstellen aus, etwa über täuschend echte E-Mails oder vertrauenswürdig wirkende Nachrichten.

Auch künstliche Intelligenz spielt im Bereich der IT-Sicherheit eine doppelte Rolle: Einerseits hilft sie dabei, Bedrohungen frühzeitig zu erkennen und Anomalien im Systemverhalten zu identifizieren. Andererseits nutzen Angreifer KI, um ihre Methoden weiter zu verfeinern – etwa durch besonders glaubwürdige Phishing-Nachrichten, automatisierte Angriffe oder die gezielte Ausnutzung von Schwachstellen. Entsprechend wichtig ist es, Sicherheitsstrategien laufend anzupassen, zu testen und weiterzuentwickeln.

Denn die Risiken im Netz entwickeln sich rasant – und mit ihnen die Angriffsmethoden. Eine aktuelle Studie zeigt: Im Jahr 2024 waren weltweit rund 63 Prozent der Unternehmen von Ransomware-Angriffen betroffen, wobei die weltweiten Gesamtschäden auf geschätzte 60 bis 120 Milliarden Euro beziffert werden – Tendenz steigend.

Christian Pfeifer

© Alle Rechte vorbehalten

Worauf es bei der Cyberbedrohung auch für kleine und mittlere Südtiroler Unternehmen ankommt?

Der oft zu niedrige (und deshalb gefährliche) Risikoeinschätzung der eigenen Verwundbarkeit. Gerade kleinen und mittleren Unternehmen (KMU) wird häufig suggeriert, sie seien für Hacker nicht interessant. Tatsächlich zeigen die Vorfälle der letzten Monate jedoch das Gegenteil: Die Angriffe erfolgen zunehmend automatisiert, großflächig und ohne vorherige Auswahl. Es ist längst nicht mehr die Frage, ob ein Unternehmen Ziel eines Angriffs wird, sondern wann.

Ein weiterer, oft übersehener Faktor ist die Verwendung veralteter Systeme und Software. Sicherheitslücken, die bereits seit längerem bekannt sind, werden von Angreifern systematisch ausgenutzt – insbesondere dann, wenn Updates nicht zeitnah eingespielt werden. Hinzu kommt der Mensch: Phishing, also der Versuch, über täuschend echte E-Mails an sensible Daten zu gelangen, bleibt eine der häufigsten und wirksamsten Methoden. Regelmäßige Schulungen und ein geschärftes Bewusstsein im Team sind daher ein zentraler Baustein der Prävention.

Nicht zuletzt spielen auch eine klare Notfallplanung und regelmäßige Back-ups eine entscheidende Rolle. Nur wer vorbereitet ist, kann im Ernstfall schnell reagieren, den Schaden begrenzen und den Geschäftsbetrieb möglichst rasch wieder aufnehmen.

Welche sind derzeit die größten Cybergefahren für Unternehmen?

Aktuell ist die mit Abstand am bedrohlichsten: Ransomware. Dabei handelt es sich um Schadsoftware, die Daten verschlüsselt und erst nach Zahlung eines Lösegelds wieder freigibt. Die Angriffe sind heute hochprofessionell organisiert, laufen oft vollautomatisiert und können in kurzer Zeit große Teile eines Unternehmens lahmlegen.

Eine zweite große Gefahr sind Phishing-Angriffe, die durch den Einsatz von KI immer glaubwürdiger werden. Die E-Mails wirken täuschend echt, sind sprachlich überzeugend formuliert und schwerer zu erkennen als früher.

Auch Angriffe auf Lieferketten nehmen zu: Cyberkriminelle nutzen gezielt Schwachstellen bei externen Dienstleistern oder Software-Anbietern, um darüber in die Systeme anderer Unternehmen vorzudringen. Dadurch können selbst gut geschützte Betriebe indirekt betroffen sein.

Nicht zuletzt steigt die Gefahr durch Datenlecks und unzureichend geschützte Cloud-Umgebungen. Wenn Daten versehentlich offen zugänglich sind oder Zugriffsrechte nicht sauber verwaltet werden, können Angreifer sensible Informationen abgreifen, verändern oder veröffentlichen – mit erheblichen wirtschaftlichen und reputationsbezogenen Folgen.

Welche Folgen machen Unternehmen am häufigsten zu schaffen?

Der größte Fehler ist, die Gefahren zu unterschätzen und zu glauben, dass es das eigene Unternehmen schon nicht treffen wird. Viele Firmen gehen davon aus, zu klein oder zu unbedeutend zu sein – doch die Realität zeigt etwas anderes: Gerade kleine und mittlere Unternehmen werden zunehmend ins Visier genommen, oft sogar gezielt, weil sie im Vergleich zu großen Konzernen häufig weniger gut geschützt sind.

Ein weiteres Risiko ist eine unzureichende Vorbereitung. Dazu gehört, dass keine klaren Prozesse für den Ernstfall definiert sind, etwa wie im Falle eines Angriffs zu kommunizieren ist, welche Systeme zuerst wiederhergestellt werden müssen oder wer im Unternehmen die Verantwortung übernimmt.

Hinzu kommt der teilweise fehlende Überblick über die eigene IT-Landschaft. Wenn nicht genau bekannt ist, welche Systeme, Daten und Zugriffe tatsächlich vorhanden sind, wird es schwierig, Schwachstellen zu erkennen und gezielt zu schließen.

Schließlich sind auch unzureichende Ressourcen ein häufiger Stolperstein: IT-Sicherheit wird in vielen Unternehmen noch immer als reines Technikthema gesehen und nicht als strategische Aufgabe, die Zeit, Budget und kontinuierliche Aufmerksamkeit erfordert.

Auf welche Maßnahmen sollten Unternehmen unbedingt achten?

Die Grundlage ist eine ganzheitliche und gut durchdachte Sicherheitsstrategie. Dazu gehören technische Maßnahmen wie aktuelle Systeme, regelmäßige Updates und eine mehrstufige Absicherung. Genauso wichtig ist jedoch der menschliche Faktor: Mitarbeitende sollten regelmäßig geschult werden, um Phishing-Versuche und andere Angriffsversuche frühzeitig zu erkennen.

Ein zentrales Element ist zudem ein verlässliches Back-up-Konzept: Daten sollten regelmäßig gesichert und getrennt vom Hauptsystem aufbewahrt werden, damit sie im Ernstfall schnell wiederhergestellt werden können.

Darüber hinaus empfiehlt es sich, Zugriffsrechte klar zu regeln und nach dem Prinzip des „Need-to-know" zu vergeben – also nur jene Berechtigungen, die tatsächlich benötigt werden.

Nicht zuletzt ist es wichtig, den Ernstfall zu planen und regelmäßig zu üben: Mit einem Notfallplan, klaren Verantwortlichkeiten und definierten Abläufen können Unternehmen im Falle eines Angriffs schneller reagieren und die Auswirkungen deutlich begrenzen.