Südtiroler
Wirtschaftszeitung
Wochenblatt für Wirtschaft und Politik

Tiratura: 4.500 | **Diffusione:** 18.000
Data: 18/11/2022 | **Pagina:** 2
Categoria: Raiffeisen-Geldorganisation Print & Web

Gefahr aus dem Netz

IT-SICHERHEIT – Cyberangriffe auf Betriebe nehmen zu. Die Schäden können sehr groß sein, und treffen kann es kleine Unternehmen genauso wie große. **Was man über Cyberkriminalität wissen muss,** was im Notfall zu tun ist, wo die Schwachstellen liegen – **und wie man sich schützen kann.**

Bozen – Laut Martin Galler haben Cyberangriffe auf Unternehmen in den letzten Jahren stark zugenommen.


Martin Galler

„Auch die erfolgreichen Angriffe. Denn die Angreifer suchen gezielter nach verwundbaren Computersystemen. In der Öffentlichkeit hört man dazu nur wenig, weil Betroffene nicht darüber reden wollen", sagt der Experte für Informationssicherheit beim IT-Dienstleister Konverto.

Wie läuft ein klassischer Cyberangriff ab? Richard Tappeiner, Fachexperte beim IT-Dienstleister systems, spricht von zwei Arten: einem willkürlichen und einem gezielten Angriff.

Bei einem willkürlichen Angriff handle es sich meist um standardisierte und automatisierte Angriffsmethoden. Bestes Beispiel sei eine Phishing-Mail, die an eine große Anzahl von Empfängern gleichzeitig geschickt wird: Klickt ein:e Mitarbeiter:in auf einen Link oder Anhang in der E-Mail, die täuschend echt nach einem seriösen Absender aussieht, könne der Angreifer im System des Betriebes Schadsoftware infiltrieren und Zugriff auf Daten erhalten.

„Bei einem gezielten Angriff hingegen hat der Hacker ein konkretes Ziel ausgemacht, das er mit verschiedenen Methoden zu erreichen versucht", erklärt Tappeiner. Als mögliches Ziel nennt er etwa Geschäftsunterbrechungen, indem Websites über eine Flut an Anfragen lahmgelegt werden. Diebstahl von Daten – etwa von Unternehmensgeheimnissen – könne ein weiteres Angriffsziel sein. Oder die Manipulation von Daten, um Statistiken, Studien oder Geschäftsergebnisse zu verfälschen. Häufig finde auch Erpressung statt: Der Angreifer verlangt Lösegeld und verspricht, bei Zahlung den Schlüssel für die Datenwiederherstellung herauszugeben oder gestohlene Dokumente nicht zu veröffentlichen.


Richard Tappeiner

„Hat der Angreifer seine Strategie definiert, versucht er Schritt für Schritt und mit verschiedenen Methoden, die Sicherheitsvorkehrungen auszuhebeln und ins System zu gelangen", so Richard Tappeiner.

Verhängnisvoller Klick

Die häufigsten Angriffe sind die willkürlichen über Phishing-Mails, sagen die IT-Experten. „Klickt ein Mitarbeiter in einer entsprechenden E-Mail auf einen Link, könnte am darauffolgenden Tag das Computersystem nicht mehr funktionieren, sodass der Betrieb oder ein Teil davon stillsteht. Auf dem Bildschirm des kontrollierenden Technikers erscheint dann oft die Meldung, man sei Opfer eines Angriffs geworden, müsse Lösegeld zahlen und solle sich an eine bestimmte E-Mail-Adresse wenden", schildert Martin Galler von Konverto einen klassischen Ablauf.


Foto: Shutterstock
Internetkriminalität kann jeden treffen

In der Folge gelte es, das gesamte IT-System vom Internet zu trennen und den Schaden mit einem Experten oder einer Expertin zu analysieren. Anschließend gehe es um die Wiederherstellung der Daten. „Das System wird komplett wiederhergestellt, sofern man die Sicherungsdaten hat. In letzter Zeit zielen Angriffe deshalb darauf ab, die Sicherungen zu zerstören, sofern sie zugänglich sind", merkt Galler an.

Die Wiederherstellung sei eine komplexe Angelegenheit: Da man nicht genau wisse, wie lange der Cyberangriff bereits dauert – es könne sich um mehrere Tage handeln –, wisse man auch nicht sofort, welche die letzte „saubere" Sicherung war. Diese ausfindig zu machen, sei ein großer Arbeitsaufwand, sagt IT-Fachmann Galler. Zu berücksichtigen sei auch, dass alle Systeme eines Unternehmens den gleichen Datenstand haben und die verschiedenen Anwendungen mit diesem wieder korrekt starten können.

Die effektive Datenwiederherstellung sei, abhängig von der Datenmenge, wiederum sehr zeitintensiv.

INFO

Ein Südtiroler Fallbeispiel

Martin Galler von Konverto berichtet von einem Cyberangriff auf ein Südtiroler Unternehmen, bei dem er die Wiederherstellung der Daten betreut hat. Demnach fand der Angriff über ein Wochenende statt. Nachdem sich die Schadsoftware ausbreitete, wurden am Montagabend und am Dienstag die Daten aus dem Computersystem kopiert. In der Nacht auf Mittwoch wurden die Server gelöscht und die Daten verschlüsselt, sodass am Tag darauf keine Arbeit mehr möglich war.

„Wir mussten das System komplett wiederherstellen – das Kopieren hat einen guten Tag gedauert. Ebenso musste überprüft werden, ob die Daten halbwegs konsistent sind. Am Montag darauf konnte die Betriebstätigkeit wieder aufgenommen werden – mit einer Datenlücke, die zum Glück nicht besonders groß war", erinnert sich Galler. Die fehlenden Daten habe das Unternehmen aufgrund vorhandener Belege richtigstellen bzw. aktualisieren können.

„Auf Lösegeldforderungen nicht eingehen"

Das nächste große Problem für betroffene Betriebe sind die durch den Cyberangriff tatsächlich verlorengegangenen bzw. verschlüsselten Daten. Soll man auf Lösegeldforderungen eingehen, um den Code zur Datenentschlüsselung zu erhalten? Martin Galler und Richard Tappeiner sind sich einig: Nein – es sei nicht zu empfehlen, Lösegeld zu zahlen.

Dass diesen Rat sehr viele nicht befolgen, zeigt die Statistik. Laut Galler wird weltweit in 60 Prozent der Fälle Lösegeld bezahlt, weil häufig keine sicheren Datenbackups vorhanden sind. Und zu rund 70 Prozent würden Lösegeldzahlungen zum Erfolg führen. „Früher lag die Erfolgsquote nur bei 50 Prozent. Das heißt, die Hälfte zahlte umsonst", weiß Galler.

Er rät, selbst dann kein Lösegeld zu zahlen, wenn Daten nicht nur verschlüsselt, sondern zuvor auch gestohlen werden – und der Dieb damit droht, die Daten zu verkaufen oder zu veröffentlichen. Diese Art der Erpressung komme immer häufiger vor. Freilich könne das eine sehr ungute Situation sein, wenn es sich um sensible Daten handelt, ist Martin Galler klar. Er weist zudem darauf hin, dass Diebstahl von personenbezogenen Daten bei den Behörden gemeldet werden muss.

> **Außerdem drängen wir darauf, das Bewusstsein der Mitarbeiter zu schärfen. Denn jeder Mitarbeiter trägt zur Sicherheit eines Unternehmens bei.**
>
> Martin Galler

„Man sollte rechtzeitig in IT-Sicherheit investieren, um das Risiko der Erpressbarkeit zu vermindern und für den Notfall vorbereitet zu sein", sensibilisiert Richard Tappeiner von systems. Mit einem technisch perfekten Backup und einem Notfallplan könne das IT-System schnell wiederhergestellt und der Schaden für das Unternehmen begrenzt werden.

Das Um und Auf für mehr IT-Sicherheit

In einer weiteren Sache sind sich Galler und Tappeiner einig: Cybersicherheit in Unternehmen müsse auf mehreren Ebenen stattfinden. Nicht fehlen dürfe etwa ein wirklich sicheres Datenbackup, das von einem Angreifer nicht gelöscht werden kann. Zu den Standardsicherheitsmaßnahmen gehöre zudem ein Malware- und E-Mail-Schutz.

„Außerdem drängen wir darauf, das Bewusstsein der Mitarbeiter zu schärfen. Denn jeder Mitarbeiter trägt zur Sicherheit eines Unternehmens bei. Jeder könnte auf einen falschen Link in einer E-Mail klicken", betont Martin Galler.

Auch Richard Tappeiner sagt: „Die Betriebe haben grundsätzlich eine hohe Bereitschaft zu Investitionen in Technologie, doch das Sicherheitsrisiko Mensch wird oft noch vernachlässigt. Die Mitarbeiter müssen ins Sicherheitskonzept integriert sein und entsprechend geschult werden. Wir als IT-Dienstleister bauen eine technisch gute Festung. Kommen die Angreifer deshalb nicht weiter, versuchen sie oft, über die Mitarbeiter in die Festung zu gelangen. Einige Phishing-Mails rutschen immer wieder durch. Und ein Klick kann große Auswirkungen haben."

Dazu merkt Martin Galler an: „Zugriffsberechtigungen sind in Unternehmen sauber einzurichten. Wenn ein Account bestimmte Tätigkeiten nicht machen muss, darf er auch nicht die Zugriffsrechte dafür haben. Denn wenn jemand Zugriff auf alles hat und auf den falschen Link klickt, könnte das ganze Unternehmen stillstehen – andernfalls womöglich nur ein Computer.

Weitere Schwachstellen bringe das Homeoffice hervor: VPN-Systeme ohne ausreichende Authentifizierungssysteme, neue Betrugsmaschen wie Fake-Einladungen zu Videokonferenzen und kein unmittelbarer Zugang zu den Sicherheitsexpert:innen im Betrieb.

„Es kann jeden treffen"

Die beiden von der SWZ befragten IT-Security-Experten sagen, Cyberangriffe auf Südtiroler Unternehmen gebe es öfter als man denkt. Durch gute Sicherheitssysteme könne man sie abwehren. Betroffen seien nicht nur größere, sondern auch kleine Betriebe. „Bei kleinen Unternehmen haben Angreifer sogar leichteres Spiel, denn sie sind weniger gut geschützt", unterstreicht Martin Galler.

Auch Richard Tappeiner weiß: „Je größer ein Betrieb, desto mehr Sensibilität hat er für Cybersicherheit und ist entsprechend besser vorbereitet. Kleinere Betriebe haben hingegen Nachholbedarf. Die Sensibilität ist zwar da, aber man muss die Kunden viel stärker überzeugen, dass auch sie betroffen sein können."

Generell haben die Südtiroler Betriebe laut Tappeiner in den letzten Jahren die IT-Sicherheit verbessert. Es gebe aber nach wie vor Investitionsbedarf, „denn die Sicherheitssysteme müssen ständig angepasst werden, da auch die Angreifer ihre Strategien ständig anpassen."

Heinrich Schwarz
heinrich@swz.it