Südtiroler
Wirtschaftszeitung
Wochenblatt für Wirtschaft und Politik

Tiratura: 4.500 | **Diffusione:** 18.000
Data: 07/07/2023
Categoria: Raiffeisen-Geldorganisation Print & Web

Schlimmer geht's immer

IT-SICHERHEIT (1) – Die Anzahl und auch der Schweregrad der Angriffe auf die IT-Systeme von Unternehmen nehmen in bedenklichem Maße zu. Unternehmen reagieren meistens, wenn es schon zu spät ist. **Wie sich Unternehmen besser schützen können** – noch bevor die Kriminellen beginnen, die KI zu nutzen.

Bozen – Es gibt nur eine Richtung: immer schlimmer! Dies ist der eindeutige Trend, welcher sich in den letzten Jahren bei der Beurteilung der IT-Sicherheit in Unternehmen abgezeichnet hat. Diese Kernaussage findet sich übereinstimmend in einschlägigen Publikationen wie dem Lagebericht des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder dem Bericht der italienischen „Associazione Italiana per la Sicurezza Informatica" (Clusit). Die Situation in unserer Region ist da sicher keine Ausnahme. Die Anzahl der erfolgreichen Angriffe auf Unternehmen ist kontinuierlich gestiegen und der Schweregrad der Angriffe hat bedenklich zugenommen.

Von der Lösegeldforderung bis zum DDoS-Angriff

Die größte Bedrohung in der Wirtschaft ist und bleibt die digitale Erpressung durch Ransomware; diese erfolgt mittlerweile in drei Steigerungsstufen: Die IT-Systeme werden durch Verschlüsselung unbrauchbar gemacht und es wird Lösegeld gefordert; kommt das Opfer dieser Aufforderung nicht nach, drohen die Erpresser, die abgegriffenen Unternehmensdaten zu veröffentlichen oder zu verkaufen; wenn das Opfer auch darauf nicht reagiert, wird mit einer Lahmlegung des Internetzugangs mittels DDoS-Angriff („Distributed Denial of Service": Massenhafter bösartiger Datenverkehr blockiert die Internetverbindungen) reagiert.

Waren solche Vorfälle vor kurzer Zeit noch eine Schlagzeile in den Medien wert, so stehen sie mittlerweile auf der Tagesordnung. Die Auswirkungen auf das Opfer sind aber nach wie vor verheerend. Über Nacht, meist über das Wochenende, wird das Unternehmen in eine tiefe Krise gestürzt, deren Bewältigung einschneidende Entscheidungen und schweißtreibenden Einsatz erfordert; nur so gelingt es, die Systeme nach einigen Tagen, Wochen oder Monaten wieder vollumfänglich verfügbar zu machen.

> **Es ist eine gewaltige Schieflage entstanden zwischen dem rasant wachsenden Angriffsarsenal der Angreifer und der behäbigen Verteidigungsreaktion der Opfer.**

Warum immer schlimmer?

Es ist eine gewaltige Schieflage entstanden zwischen dem rasant wachsenden Angriffsarsenal der Angreifer und der behäbigen Verteidigungsreaktion der Opfer.

Auf der Angreiferseite hat eine Spezialisierung stattgefunden, und die Angriffe werden arbeitsteilig durchgeführt. Da gibt es die Entwickler von Schadsoftware, die Datenhändler, die Vermieter von Angriffsplattformen, die Inkassostellen und die konkreten Initiatoren des Angriffs; der „Gewinn" wird anteilsmäßig aufgeteilt.

Auf der Seite der Opfer hingegen hat sich wenig getan. Während einige Unternehmen das Thema IT-Sicherheit nach wie vor sträflich vernachlässigen, gelangte es bei anderen richtigerweise in die Managementebene. Allerdings ist für eine wirksame Abwehr eine konsequente Umsetzung einer ganzen Reihe von Maßnahmen notwendig. Und dabei fehlt es vor allem an der notwendigen Konsequenz: Es sind Schwierigkeiten auf verschiedenen Ebenen zu bewältigen, vom Mangel an finanziellen Ressourcen über fehlendes qualifiziertes Personal bis zu Ablehnungshaltungen von einzelnen Mitarbeitenden oder Führungskräften.

Die Bearbeitung eines Ernstfalles erfolgt aber immer auf einheitliche Weise: Ohne Wenn und Aber wird eine komplett neue Infrastruktur aufgesetzt, welche zu hundert Prozent alle Sicherheitsvorkehrungen berücksichtigt. Auf diese saubere und sichere Infrastruktur werden dann die Daten, welche aus den Sicherungskopien gerettet werden konnten, wieder aufgespielt. Natürlich ist eine solche Aktion schmerzhaft und teuer, aber es gibt keinen anderen Weg. Spätestens an diesem Punkt muss man sich der Frage stellen, warum diese Maßnahmen nicht schon vorher umgesetzt worden sind. Warum ist plötzlich das möglich, was vorher nicht möglich war?

Bewährte Maßnahmen neu implementiert

Die klassischen Maßnahmen für die Abwehr und Bekämpfung sind nach wie vor sehr wirksam; aufgrund der Aufrüstung der Angreifer müssen aber einige Aktionsfelder vermehrt in den Fokus gerückt werden.

Dazu gehört selbstverständlich die regelmäßige Datensicherung. Dabei ist aber zu beachten, dass die Angreifer speziell eine Jagd auf diese Datensicherungen machen, um sie zu zerstören; deshalb ist unbedingt ein besonderer Schutz für diese Datensicherungen vorzusehen.

Alle Systeme müssen immer zeitnah aktualisiert werden, um den Angreifern keine offenen Türen zu bieten. In der Praxis wird dies zwar für einige wichtige Systeme durchgeführt, es gibt aber häufig einige ältere oder ausgemusterte Systeme, welche immer noch vor sich hinvegetieren. Dies sind dann beliebte Einfallstore für Angreifer. Hier ist also mehr Entschlossenheit für das endgültige Abschalten und Löschen notwendig.

In der Praxis wird es den Angreifern recht einfach gemacht, sich im internen Netz auszubreiten, auf sensible Daten zuzugreifen und diese auf ihre Server im Internet hochzuladen. Grund dafür ist eine viel zu laxe Implementierung der internen Zugangsregeln auf die Daten sowie der freizügige Internetzugang für die Mitarbeitenden. Eine Verbesserung dieser Regeln ist einfach durchzuführen und hat sich in konkreten Fällen immer als sehr wirksam erwiesen.

Selbstverständlich braucht es für die Sicherheit technische Hilfsmittel wie ein gut konfiguriertes Identitätsmanagementsystem, einen Schutz vor Schadsoftware und geeignete Firewall-Systeme. Jedes dieser Systeme erledigt eine spezifische Aufgabe und erzeugt zudem eine Menge von nützlichen Informationen. Diese Informationen, vor allem jene, welche mittels einer übergreifenden Sicht gewonnen werden, sind eine wertvolle Quelle, um die konkrete Bedrohungslage einzuschätzen. Damit kann ein Angriff schon in einer frühen Phase entdeckt, bekämpft und eingedämmt werden. Rund um die Uhr sollte ein professionelles „Security Operation Center" (Soc) solche Analysen vornehmen und bei Bedarf sofort einschreiten.

Der Angriff auf den Faktor Mensch

Das Sicherheitsbewusstsein aller Mitarbeitenden (Awareness) war schon immer ein unverzichtbarer Teil einer Sicherheitsstrategie und gewinnt noch an Bedeutung. Durch den Angriff auf den Faktor Mensch können alle technischen Sicherheitsfunktionen außer Kraft gesetzt werden. Es ist sogar so,

Südtiroler
Wirtschaftszeitung
Wochenblatt für Wirtschaft und Politik

Tiratura: 4.500 | **Diffusione:** 18.000
Data: 07/07/2023
Categoria: Raiffeisen-Geldorganisation Print & Web

dass durch reine menschliche Manipulation, also ohne die IT-Systeme zu verletzen, ökonomisch gesehen der größte Schaden entsteht. Bekannt sind in unserer Region viele Betrugsfälle, wo Rechnungen anstatt auf das Konto des Lieferanten auf jenes des Betrügers beglichen wurden. Gleich gelagert ist der Fall, wo der Betrüger sich vom Personalbüro das Gehalt eines bzw. einer Mitarbeitenden überweisen lässt, weil anscheinend die Bank für das Gehaltskonto gewechselt wurde. Es ist erstaunlich, wie wirksam solche Betrugsmaschen heute schon sind. Kaum auszudenken, wie erfolgreich diese sein werden, wenn sie von künstlicher Intelligenz (KI) erzeugt werden.

Ganzheitlicher Ansatz

Die erwähnten Maßnahmen stellen nur einen Auszug aus einer notwendigen ganzheitlichen Sicherheitsstrategie dar. Eine solche sollte sich auf bewährte Vorlagen stützen, wie etwa das „Cyber Security Framework" des amerikanischen „National Institute of Standards and Technology" (Nist). Dieses umfasst fünf Phasen: identifizieren der wichtigen Ressourcen, schützen dieser Ressourcen, erkennen von Angriffen, reagieren auf Ereignisse und Wiederherstellungspläne. Die Verwendung dieser Vorlage des Nist ist in Italien sehr vorteilhaft, da Teile davon bereits in die italienische Gesetzgebung eingeflossen sind.

IT-Sicherheit ist nicht Privatsache

Auch die neu gegründete Agentur für Nationale Cybersicherheit (ACN – Agenzia per la Cybersicurezza Nazionale) stützt sich bei ihren Vorschriften und Kontrollen vielfach auf die Nist-Vorlage. Diese Agentur ist gegründet worden, um alle nationalen Kompetenzen zur IT-Sicherheit zu bündeln und auf sich zu vereinen. Zu den Aufgaben der Agentur gehört neben der Förderung von Sicherheitsmaßnahmen auch die Überprüfung der IT-Sicherheit von Unternehmen. Mit der neuen europäischen Richtlinie zur Netzwerk- und Informationssicherheit (Nis2) fallen immer mehr Unternehmen unter den Kontrollbereich dieser Behörde. Aber auch ohne diese Richtlinie ist jedes Unternehmen ohnehin im Rahmen des Datenschutzes (DSGVO) verpflichtet, die Sicherheit der personenbezogenen Daten nach dem Stand der Technik zu gewährleisten. Es ist zu erwarten, dass die diesbezüglichen Kontrollen nicht mehr von der Finanzbehörde, sondern vom ACN durchgeführt werden.

Mehr Sicherheit wirkt nicht zwingend hemmend

Die fortschreitende Digitalisierung und die ansteigende Bedrohung erfordern die Schaffung einer hohen Sicherheitskultur im Unternehmen. Die Umsetzung der Maßnahmen hat unterschiedliche Auswirkungen quer durch alle Bereiche. Es ist aber nicht so, dass mit einer Erhöhung der Sicherheit zwingend eine hemmende Wirkung auf die Arbeitsabläufe einhergeht. Einige technische Errungenschaften, wie etwa die passwortlose Anmeldung, bieten da Erleichterungen, welche von den Benutzern und Benutzerinnen gerne angenommen werden. Andere Maßnahmen müssen ausgelagert und in professionelle Hände gelegt werden. Und schließlich bietet eine Analyse der notwendigen Zugriffsrechte auch die Gelegenheit, einige Abläufe neu zu gestalten und zu verschlanken.

Martin Galler

DER AUTOR
ist der Verantwortliche für „Information Security & Privacy" bei Konverto mit Sitz in Bozen.