Südtiroler
Wirtschaftszeitung
Wochenblatt für Wirtschaft und Politik

Tiratura: 4.500 | **Diffusione:** 18.000
Data: 09/07/2021 | **Pagina:** 19 | **Autore:** Simon Kofler simon.kofler@konverto.eu
Categoria: Raiffeisen-Geldorganisation Print & Web

Mehrere „Fronten“

CYBERSICHERHEIT – Die IT-Sicherheit ist angesichts neuer digitaler Arbeitsmethoden wesentlicher, um als Unternehmen erfolgreich zu arbeiten. Trotzdem besitzen nur rund 30 Prozent der italienischen Firmen eine durchdachte Sicherheitslösung. **Wie kann eine solche Lösung einfach und richtig umgesetzt werden?**

Bozen – Seit Jahren steigt die Anzahl der Cyberangriffe, und deren Gefährlichkeit nimmt stetig zu. Es stellt sich nicht mehr die Frage, ob ein Unternehmen von einem solchen Ereignis betroffen sein wird, sondern nur mehr wann. Dafür ist weder die Firmengröße noch die Mitarbeiterzahl ausschlaggebend.

Ein Cyberangriff kann für ein Unternehmen äußerst negative, zum Teil jahrelang nachwirkende Konsequenzen haben – vom Produktionsausfall über eventuelle Verluste von Kund:innen bis zum Imageschaden. Mit bestimmten Schutzmechanismen können Cyberangriffe jedoch verhindert, zumindest aber erschwert werden. Für eine effektive Sicherheitslösung sind drei Faktoren ausschlaggebend: die technische Sicherheitsinfrastruktur, das menschliche Verhalten und eine verlässliche Datensicherung.

Technischen Grundstein legen: Firewall als erste Barriere

Schadprogramme wie Viren oder Malware gelangen über Schwachstellen im Netzwerk oder durch das Klicken und Herunterladen von Dateien in das Unternehmensnetzwerk. Eine Firewall sowie Antivirus- und Filterprogramme bilden eine erste Barriere gegen Schadsoftware.

Eine Firewall überwacht den gesamten Datenverkehr zwischen dem Unternehmensnetzwerk und dem Internet. Aufgrund von festgelegten Regeln können Websites, Programme oder Netzwerke blockiert oder als vertrauenswürdig eingestuft werden.

Zusätzlich sollte ein zuverlässiges Antivirenprogramm verwendet werden. Solche Programme gleichen Inhalte auf Webseiten und Dienste mit aktuellen Virendatenbanken ab und blockieren diese oder warnen vor deren Ausführung. Außerdem sind angesichts von Spam- und Phishing-Mails Programme ein Muss, die eingehende E-Mails nach IP-Adressen, Absendern sowie Inhalten filtern und die kritische E-Mails kennzeichnen, verschieben oder löschen.

Herausforderung *Smart Working*

Die technische Sicherheitsinfrastruktur war bisher auf das Unternehmensnetzwerk beschränkt. Mit dem digitalen Aufschwung müssen die Sicherheitssysteme jedoch auch an die neuen Arbeitsmethoden der Mitarbeiter:innen angepasst werden. Das Hauptaugenmerk liegt dabei in der Absicherung des Zugangs auf die Unternehmensdaten. Traditionell spielt der Einsatz eines VPN (*Virtual Private Network*) eine wichtige Rolle. Es sollte in diesem Fall auf die Verwendung privater Geräte verzichtet werden, sodass das Gerät regelmäßig von der IT-Abteilung der:des Arbeitgeber:in auf das erforderliche Sicherheitsniveau aktualisiert und besser geschützt werden kann.

Mit dem standortungebundenen Arbeiten und flexiblem Einsatz von Geräten bietet sich der Zugang zu Unternehmensdaten über verschiedene Cloud-Applikationen an. Hierbei wird der gesamte Datenaustausch verschlüsselt, sodass sensible Informationen nicht von Unbefugten ausgelesen werden können. Ein modernes Anmeldesystem zur Identifizierung der:s Mitarbeiter:in ist unumgänglich. Idealerweise sollte auf eine Multi-Faktor-Authentifizierung gesetzt werden. Diese nutzt die Kombination von mehreren Identitätsnachweisen, die auf biometrischen Merkmalen, speziellem Wissen oder einem mitgeführten Gegenstand basieren und voneinander unabhängig sind (beispielsweise Fingerabdruck und einmalig nutzbarer Code auf einem Handy).

Entscheidend für alle technischen Sicherheitsinfrastrukturen, sei es am Unternehmenssitz oder im *Smart Working*, ist die laufende Anpassung und Aktualisierung, sodass Angriffe optimal abgewehrt werden können.

Entscheidender Faktor Mensch

Einen weiteren wesentlichen Aspekt darf ein ganzheitliches Sicherheitskonzept nicht vernachlässigen: Der Faktor Mensch ist häufig das schwächste Glied der Kette.

Durch gezielte Manipulation von Menschen ist es möglich, alle technischen Sicherheitsmaßnahmen außer Kraft zu setzen. Hacker und Datendiebe entwickeln kontinuierlich neue Angriffstechniken, welche genau darauf abzielen, und imitieren legitimes Verhalten so genau, dass eine eindeutige Unterscheidung fast unmöglich ist. Beim *Social Engineering* etwa nutzen Hacker persönliche Informationen der Mitarbeiter:innen aus, um an vertrauliche Informationen zu kommen.

In der Regel ist nur ein kleiner Teil der Mitarbeiter:innen in der Lage, einen Angriffsversuch zu erkennen und bewusst darauf zu reagieren. Mit *Security Awareness Trainings* kann man dieser Situation entgegenwirken. Ziel ist es, ein nachhaltiges Sicherheits- und Risikobewusstsein im Unternehmen zu erreichen.

Absicherung hoch drei

Sind diese Vorkehrungen getroffen, ist ein erfolgreicher Angriff um Einiges unwahrscheinlicher. Nichtsdestotrotz sollte ein Unternehmen immer auf ein vollständiges und ausfallsicheres Backup zurückgreifen können, denn nur ein solches ermöglicht die Wiederherstellung von gestohlenen oder blockierten Daten.

Die Grundlage eines sicheren Datenback-ups ist die 3-2-1-Regel. Nach dieser sollten stets drei Kopien der Unternehmensdaten existieren; zwei Kopien werden auf unterschiedlichen lokalen Medien gespeichert und die letzte Kopie in der Cloud aufbewahrt. Aufgrund der großen Datenmengen und komplexen Netzwerkumgebungen scheinen Backups auf den ersten Blick zwar kompliziert, doch mit vollautomatisierten Lösungen gestaltet sich diese Aufgabe einfacher als gedacht. Sie kann bei Bedarf auch von einem Servicepartner übernommen werden.

Simon Kofler
© simon.kofler@konverto.eu

DER AUTOR ist *Head of Operation Center Security* bei KONVERTO. Der Südtiroler IT-Dienstleister veranstaltet am 22. Juli (14 bis 18 Uhr) in der Kellerei St. Michael/Eppan den Event *talks Operating Security* zum Thema Cyber-Sicherheit. Info und Anmeldung unter talks.konverto.eu.