Südtiroler Wirtschaftszeitung
Wochenblatt für Wirtschaft und Politik

Dieser Artikel ist in der Ausgabe erschienen: Nr. 19/19 | Freitag, 10. Mai 2019

Digital

Schwachstelle Mensch

IT-Sicherheit – Die Cyberkriminalität nimmt zu, doch viele Unternehmen unterschätzen weiterhin die Gefahr. Dabei haben Hacker weltweit ihre Strategie geändert. Sie greifen nun meist nicht mehr über das System an, sondern über eine viel größere Schwachstelle, die in jedem Unternehmen zu finden ist: den Menschen.

Bozen – Keine drei Wochen ist es her, dass Hotelbetriebe im Schlerngebiet Opfer von Cyberangriffen geworden sind. Die Täter hatten sich durch vireninfizierte E-Mails, sogenannte Trojaner, Zugang zu den Hotelcomputern verschafft. Für die gestohlenen Daten forderten sie anschließend Lösegeld. Immer wieder warnt die Postpolizei vor verdächtigen E-Mails und gibt Tipps:

- E-Mails gründlich lesen und prüfen;
- Anhänge nur von verifizierten Absendern öffnen;
- Adressen und andere Daten regelmäßig schützen;
- Antivirusprogramm stets auf dem neuesten Stand halten.

Malware, also unerwünschte bzw. schädliche Programme, sind nur ein kleiner Teil der Cyberkriminalität. Daten sind mittlerweile zum wertvollsten Rohstoff der Welt geworden, dementsprechend versuchen immer mehr Menschen, sich daran zu bereichern – auf legale oder eben auf illegale Weise. Warren Buffet, US-amerikanischer Großinvestor, geht so weit zu sagen: „Ich denke, Cyberattacken sind das größte Problem der Menschheit."
Wie verbreitet Cyberattacken bereits sind, zeigt eine Studie des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien (bitkom) vom September 2018. Ihr zufolge wurden sieben von zehn deutschen Unternehmen in den vergangenen zwei Jahren Opfer von Cyberattacken oder Industriespionage. Die dadurch entstandene Schadenssumme wird auf 43,4 Milliarden Euro geschätzt. Weltweit sollen die Schäden durch Cybercrime bis 2021 auf sechs Billionen Dollar steigen, das ist eine Verdoppelung der drei Billionen Dollar im Jahr 2015, so eine Studie des Marktbeobachters Cybersecurity Ventures.

Südtiroler
Wirtschaftszeitung
Wochenblatt für Wirtschaft und Politik

Obwohl sich Datendiebstahl, digitale Sabotage und Co. häufen, ist das Thema Cybersicherheit nach wie vor für die meisten Menschen wenig greifbar und wird häufig unterschätzt. Gerade kleinere Unternehmen sind dankbare Ziele für Betrüger, da sie oft nicht ausreichend geschützt sind. Derzeit würden sich in Südtirol zwei Methoden häufen, mit denen Unternehmen Opfer von Cyberkriminalität werden, sagt Ivo Plotegher von der Postpolizei. Diese nutzen die Technik des Social Engineerings, das heißt, Menschen werden von den Betrügern gezielt manipuliert und für ihre Zwecke instrumentalisiert. Die Hacker nutzen das fehlende technische Wissen der Benutzer. Während früher oft direkt das System angegriffen wurde, beinhaltet heute beinahe jede Art von Angriff ein gewisses Maß an Social Engineering.
Die erste in Südtirol weit verbreitete Masche, sagt Plotegher, mache sich die Geschäftsbeziehungen zu anderen Firmen zunutze: Im Unternehmen trudelt die E-Mail eines langjährigen Lieferanten ein. Der Lieferant habe seine IBAN geändert. Das Unternehmen überweist die Rechnung in der Folge auf diese neue IBAN, stellt dann aber fest, dass die E-Mail gar nicht vom Lieferanten, sondern von einem Betrüger kam. „Erhält man eine derartige E-Mail, sollte man einfach zum Hörer greifen und kurz nachfragen, ob die IBAN tatsächlich geändert wurde“, rät Plotegher. Ist das Geld nämlich einmal weg, bekomme man es in den seltensten Fällen wieder.
Eine zweite Masche ziele auf interne Abläufe: Ein Mitarbeiter, der für die Rechnungsabwicklung zuständig ist, erhält vermeintlich eine E-Mail vom Geschäftsführer mit der Bitte, eine Überweisung auf ein bestimmtes Konto vorzunehmen. Auch in diesem Fall steckt ein sogenannter Social Engineer dahinter, der im Internet nach geeigneten Opfern sucht. „Hier raten wir, interne Abläufe so zu gestalten, dass es eine Gegenkontrolle gibt“, sagt Plotegher. Der Schutz vor Social Engineering beginnt im Allgemeinen mit Weiterbildung. „Denn das beste System“, sagt Peter Nagler, Direktor des Raiffeisen-IT-Dienstleisters Konverto, „nützt nichts, wenn Mitarbeiter Hackern die Tür öffnen.“ (Siehe dazu auch beistehendes Interview.)

Sabina Drescher
sabina@swz.it

Infobox
Die Tür geht auch von innen auf
SWZ: Wie wichtig ist Cybersicherheit für eine erfolgreiche Digitalisierung?
Peter Nagler*: Die Cybersicherheit ist grundsätzlich enorm wichtig, unabhängig vom Digitalisierungsgrad eines Unternehmens. Allein wenn ich das Internet nutze, ist die Wichtigkeit schon enorm hoch. Rein gesetzlich braucht jedes Unternehmen Internetverbindung zum elektronischen Datenaustausch und muss sich folglich schützen. Im Grunde geht es bei der Cybersicherheit stets um die Frage: Wie kann ich richtig vorsorgen?

Wie weit haben die Unternehmen bei uns im Land schon vorgesorgt?
Ich sage mal so: Die Situation ist etwas durchwachsen. Wenn man einen Unternehmer fragt, zeigt er sich von der Wichtigkeit des Themas überzeugt und ist sich auch sicher, dass sein Betrieb ausreichend geschützt ist. In der Praxis sieht es dann aber oft anders aus. Unternehmen sind gesetzlich verpflichtet, aktuelle Antivirenprogramme auf ihren Rechnern zu installieren. Es gibt auch Strafen bei Nichteinhaltung. Trotzdem findet man Unternehmen, die diesen Standard nicht einhalten. Manche Rechner werden vergessen, manchmal ist nicht klar, wer für die Wartung zuständig ist, in anderen Fällen ist die Software veraltet. Viele kennen die Gefahren nicht, die dahinterstecken können.

Wieso wird das Thema oft noch stiefmütterlich behandelt?
In den seltensten Fällen liegt es an der ökonomischen Seite. Vielfach ist es die Unwissenheit darüber, was passieren kann. Wir erleben auch, dass Kunden der Meinung sind, dass ein Programm installiert wurde, obwohl dem nicht so ist. Sie glauben sich geschützt, sind es de facto aber nicht. Insbesondere der Faktor Mensch wird vielfach unterschätzt.

Welche Rolle spielen denn die Mitarbeiter?
Hacker, Trojaner usw. konzentrieren sich heute nicht mehr vordergründig darauf, direkt in die Systeme einzudringen, sondern versuchen, die Gutmütigkeit der Mitarbeiter auszunutzen. Es werden Mails oder Links mit schädlichen Inhalten verschickt, die Mitarbeiter aber lösen den Angriff erst aus, indem sie zum Beispiel irgendwo draufklicken. Das passiert häufiger, als man meint. Früher galt: Ich muss mich von außen abschotten, damit kein Fremder reinkommt. Heute ist es anders. Viele Leute sind sich noch nicht bewusst, dass die Tür auch von innen nach außen aufgeht. Das ist die große Änderung im Vorgehen von Hackern im Allgemeinen.

Ihre Tipps für Unternehmen?
Ein Punkt sind die Investitionen in die Systeme und Schutzmechanismen. Mindestens gleich wichtig sind die Sensibilisierung und Schulung der Mitarbeiter. Was kann passieren, was sind Gefahrenquellen, und welche Auswirkungen können Cyberangriffe haben? Wenn ein Mitarbeiter die Tür aus Unwissenheit oder Unachtsamkeit öffnet, nützt mir das beste System nichts.

** Peter Nagler ist Direktor des Raiffeisen-IT-Dienstleisters Konverto.*