

«Die Angriffsfläche wächst und wächst»

Rapperswil-Jona In der Privatwirtschaft sind Cyberattacken an der Tagesordnung. Ivan Bütler, Geschäftsführer der Compass Security in Rapperswil, testet und berät seine Kunden bezüglich Sicherheit im Netz.

Herr Bütler, im letzten Jahr haben die Hacker-Angriffe auf die öffentlichen Verwaltungen Montreux und Rolle für Aufsehen gesorgt. Dabei wurden Daten gestohlen und ins Darknet gestellt. Sind das Einzelfälle oder erkennen Sie da einen Trend?

Es ist in der jüngeren Vergangenheit tatsächlich eine Häufung solcher Angriffe zu erkennen. Mir kommen da ganz spontan noch der Angriff auf die Gemeinde Rorschach und zuletzt auf die Website des Kantons und der Stadt St. Gallen im Oktober in den Sinn. Es kann aber durchaus auch bundesstaatliche Institutionen treffen, wie etwa die Fälle der Ruag oder des Seco gezeigt haben.

Ähneln sich die Angriffe?

Man muss zwischen gezielten Attacken und Attacken nach dem Giesskannenprinzip unterscheiden. Bei ersteren geht es vor allem darum, ganz bestimmte Informationen zu stehlen, die man im Markt monetarisieren und beispielsweise im Bereich der Spionage oder zu Forschungszwecken verwenden kann. Letztere werden indessen breit gestreut, mit dem Ziel, Datenträger zu verschlüsseln und danach Lösegeld zu erpressen.

Welcher Bedrohungstyp ist für die kommunale Verwaltung gefährlicher?

Klar letzterer. Diese sogenannten Ransom-Angriffe, die man in der Privatwirtschaft schon lange kennt, sind darauf ausgerichtet, möglichst grossen Schaden anzurichten, um maximalen Druck auszuüben. Natürlich, auf kantonaler Ebene kann es ebenfalls gezielte Angriffe geben, wenn mit den gestohlenen Daten Geld verdient werden kann; etwa mit Steuerausgängen, die man einem anderen Staat verkaufen könnte. Doch auf der kommunalen Ebene sind Ransom-Angriffe einträglicher.

Hacker gelten als enorm dynamisch. Sind bereits neue Trends absehbar?

Wir sehen in der Privatwirtschaft Vorgehensweisen, die den Kausalzusammenhang zwischen dem Diebstahl und der Monetari-

sierung brechen wollen. So sind Fälle bekannt geworden, bei denen Hacker die Quartalsberichte von börsenkotierten Firmen kurz vor deren Präsentation entwendet und dann mittels Komplizen an der Börse hochprofitable Insidergeschäfte getätigt haben. Ähnliches haben wir in der Verwaltung zwar noch nicht beobachtet, es wäre aber durchaus denkbar – zum Beispiel bei Patienten.

Die Pandemie wird gerne als Katalysator dieser Kriminalität bezeichnet. Einverstanden?

Ja und nein. Es stimmt natürlich insofern, als dass das forcierte Homeoffice-Modell mehr einzelne Angriffspunkte geschaffen hat. Es ist aber vielmehr die ganze Digitalisierung an sich, die den Hackern neue Felder öffnet. All unsere Lebensbereiche werden derzeit von dieser erfasst, es gibt deshalb Unmengen an neuen Projekten.

Umso wichtiger sollte also auch der Aspekt Sicherheit werden.

Das ist so. Oft wird aber immer noch der Fehler gemacht, dass zuerst ausschliesslich auf die Funktionalität und erst zum Schluss auf die Sicherheit geschaut wird. Ein ganz prominentes Beispiel wäre hier das Projekt «Meineimpfungen.ch», das einen elektronischen Impfausweis schaffen sollte. Es musste wegen gravierender Sicherheitsmängel wieder vom Netz genommen und die dazugehörige Stiftung liquidiert werden.

Sind wir der Aufbruchsstimmung wegen generell zu forscher?

Das würde ich so nicht sagen. Fakt ist aber, dass der Mensch die Konsequenzen der Technologie oft nicht versteht. Das Feld, das sich uns eröffnet, ist riesig, die Angriffsfläche wächst und wächst. Grosse Firmen wie Microsoft bemühen sich bezüglich Sicherheit enorm. Doch der Dschungel ist weit und dicht.

Ihre Firma Compass Security prüft regelmässig die IT-Sicherheit von Firmen, aber auch von öffentlichen Verwaltungen, u.a. im Zürcher Oberland. Wie gehen Sie dabei vor?

Wir stellen einen Schlachtplan zusammen und vereinbaren mit den Kunden einen Zeitraum, in dem wir seine Systeme hacken. Dabei erkennen wir die Schwachstellen, für deren Behebung wir einen Massnahmenkatalog erstellen. Diesen stellen wir dem Auftragsgeber und dessen IT-Provider zur Verfügung. Einige Monate später machen wir schliesslich einen Re-Test, um die Wirkung der Massnahmen zu überprüfen.

Wo finden Sie diese Schwachstellen?

Faktisch gibt es zwei Wege in ein System. Der eine führt über die Technik, der andere über den Menschen. Bei ersterer kann man über Schnittstellen und Lächer eindringen. Beispiele wären hier



Ivan Bütler von Compass Security mit Sitz in Rapperswil hackt von Berufs wegen die Systeme seiner Kunden. Archivfoto: Seraina Boner

die Software zum Ausfüllen der Steuererklärung oder Zahlungskonten bei Online-Plattformen. Weil die Technik aber in der Regel gut gewartet und geschützt wird, ist der Faktor Mensch für die Kriminellen weit vielversprechender. Die Angreifer gehen zuweilen so raffiniert vor, dass sie

tig sind durch die Digitalisierung so viele Bereiche betroffen, dass sich immer mehr Türen öffnen. Da geht gerne auch mal was vergessen.

Können Sie uns ein Beispiel nennen?

Das Schulwesen. Nicht selten ist

wieder Risiken. So gibt es da und dort immer noch Schulcomputer, die mit dem Schulnetz verbunden sind, an die sich jeder hinsetzen kann.

Ihre Firma bietet auch Schulungen für Mitarbeiter an. Worauf müssen Sie dabei achten?

Wichtig ist vor allem, dass wir die Leute erreichen. Man muss sich bewusst sein, dass dieses Thema für viele Leute eine Blackbox ist. So ähnlich wie der Strom, bei dem viele auch nur wissen, dass er aus der Steckdose kommt. Wir versuchen deshalb live zu zeigen, was bei einem Angriff passiert und wie man gewisse Gefahren, etwa ausführbare Dateien oder Makros, erkennt. Weiter schauen wir, dass wir den Leuten Wissen mitgeben können, von dem sie auch in ihrer privaten digitalen Welt profitieren können. Und nicht zuletzt verfolgen wir dabei unterhaltende und partizipative Ansätze, sogenanntes «Edutainment». Damit maximieren wir die Wahrscheinlichkeit, dass etwas haften bleibt.

Matthias Müller

Belimo baut Kapazitäten in Hinwil aus

Hinwil Es läuft rund bei Belimo, dem Hersteller für Antriebs-, Ventil- und Sensorlösungen. So rund, dass er jetzt den Ausbau seiner Kapazitäten am Hauptsitz in Hinwil bekannt gibt. Für das Geschäftsjahr 2021 weist Belimo ein zweistelliges Umsatzwachstum in allen Marktregionen aus. Laut einer Mitteilung profitierte die Gruppe von einer starken Nachfrage, die sie durch ihr Lieferkettenmanagement auch bedienen konnte.

Der Nachholbedarf im zweiten Corona-Jahre habe die beiden langfristigen Wachstumstreiber – die Verbesserung der Energieeffizienz des weltweiten Gebäudebestands und die erhöhten Anforderungen an die Raumluftqualität in Gebäuden – weiter verstärkt.

Boom in Europa und Amerika

Insgesamt konnte Belimo den Nettoumsatz in Lokalwährungen um 16,6 Prozent steigern. In Schweizer Franken erhöhte sich der Nettoumsatz um 15,7 Prozent auf 765,3 Millionen. Die positive Marktentwicklung habe vor allem in Europa und Amerika für eine verstärkte Nachfrage gesorgt. Für die Marktregion Europa betrug das Umsatzwachstum in Lokalwährungen 15,9 Prozent, für Amerika 18,1 Prozent.

In der Marktregion Asien-Pazifik belief sich der Anstieg auf 14,4 Prozent. Die Nettoumsätze der Luftanwendungen wuchsen in Lokalwährungen um 15,5 Prozent, diejenigen der Wasseranwendungen um 17,9 Prozent.

Schon Grundstück gekauft

Infolge des Wachstums kommt der ohnehin geplante Kapazitätsausbau schneller voran als ursprünglich geplant, wie Belimo schreibt. Über die nächsten Jahre werde man die Kapazitäten in der Produktion, Logistik und Customization mit höheren Investitionen in allen Marktregionen erweitern.

Davon profitiert auch der Standort Hinwil. Auf Nachfrage dieser Zeitung heisst es, dass man einen Kaufabsichtsvertrag für ein Grundstück in unmittelbarer Nähe zum bestehenden Gebäude unterzeichnet habe. Damit sollen Erweiterungen in Logistik und Customizing Rechnung getragen werden. Um welches Grundstück es sich handelt, will Belimo erst dann offenlegen, wenn die Transaktion abgeschlossen. Dies werde voraussichtlich im Februar erfolgen.

Zudem seien in der Marktregion Amerika am Standort Danbury (USA) die Kapazitäten in der Logistik erweitert worden, um Platz für künftiges Wachstum zu schaffen und weiterhin eine hohe Liefertermintreue zu gewährleisten.

In der Marktregion Asien-Pazifik hat Belimo den bestehenden Standort in Schanghai (China) gekauft, um zusätzliche Kapazitäten und Flächen für Lagerung, Customizing, Logistik und Büros bereitzustellen. *jöm*

Zur Person

Ivan Bütler (51) ist Gründer und Geschäftsführer von Compass Security mit Sitz in Rapperswil-Jona. Das IT-Unternehmen gehört zu den führenden Schweizer Anbietern im Bereich der Prävention und Aufklärung von Cyber-Attacken. Es beschäftigt rund 60 Mitarbeiter an den Standorten Jona, Zürich und Bern sowie in Berlin und Toronto. Bütler hat sich international einen Namen als Experte für Cyber-Security gemacht und tritt mit einschlägigen Publikationen und Vorträgen an die Öffentlichkeit. Er unterrichtet an der Fachhochschule Rapperswil und an der Hochschule Luzern. *jöm*

«Fakt ist, dass der Mensch die Konsequenzen der Technologie oft nicht versteht.»

auch Profis austricksen können.

Ist man sich dem bei den Verwaltungen bewusst?

Ich denke schon. Man muss aber schon sehen, dass es auch um Verhältnismässigkeiten geht, insbesondere hinsichtlich der Kosten. Auf einer Gemeinde gibt es sensiblere und weniger sensible Daten – die Schutzprioritäten sind unterschiedlich. Gleichzei-

es vorgekommen, dass in den 90er- und Nuller-Jahren in einem Schulhaus ein engagierter Lehrer oder ein Amateur ein erstes Netz aufgebaut hat. Das war für jene Zeit absolut ausreichend. Doch unterdessen funktioniert alles digital, alle Schulen sind miteinander vernetzt. Obschon versucht wird, Schritt zu halten, birgt ein System, an dem so viele Akteure beteiligt sind, immer

Die nächste Ausgabe



erscheint am 11. März 2022