«Angst, Schrecken und Panik»

Nach dem Cyberangriff auf Huber+Suhner geht ein Experte von erheblichen Mängeln in der IT-Sicherheit aus.

«Angst, Schrecken und Panik» – danach riecht es bei Huber+Suhner nach Einschätzung von Nicolas Mayencourt. Der Gründer und Chef der Dreamlab Technologies AG, die seit 20 Jahren Sicherheitslösungen für gefährdete IT-Infrastrukturen entwickelt und realisiert, stützt seine Beurteilung auf zwei Faktoren: Erstens hat laut Mitteilung von Huber+Suhner die zentrale IT des Technologiekonzerns sämtliche Arbeitsstationen global deaktiviert, unmittelbar nachdem interne Überwachungsdienste den Angriff mit Schadsoftware auf die IT-Systeme festgestellt hatten. Zum anderen wurde, weil auch zentrale Systeme betroffen seien, «die Produktion in sämtlichen Werken weltweit unterbrochen».

Mayencourt folgert daraus: Die unbekannten Hacker sind in Huber+Suhners IT-Systeme eingedrungen, richteten Schaden an und dieser wurde mutmasslich immer grösser. In der Folge ging es beim Unternehmen um eine Güterabwägung, wie Mayencourt sagt: «Bekommen wir das Problem in den Griff oder ziehen wir den Stecker?» Bei Huber+Suhner war der Entscheid: Stecker ziehen. Oder, wie es Mayencourt auch sagt: «Die Notfallorganisation hat die Minderung des Schadens an der Infrastruktur priorisiert.» Ob das übereilt war oder nicht, werde sich erst im Nachhinein zeigen. Firmensprecher Patrick Köppe schreibt aber auf Anfrage: «Es ging unmittelbar auch darum, weiteren möglichen Schaden abzuwenden.»

Der Cyberangriff hat Huber+Suhner den Stecker gezogen, auch im Werk in Herisau. Bild: Ralph Ribi

«Das kann einen Betrieb Kopf und Kragen kosten»

Immerhin, sagt Mayencourt, habe Huber+Suhner mit diesem Vorgehen «Zeit gewonnen und Ruhe reingebracht». Das sei auch nötig zur Spurensicherung im Rahmen der forensischen Analyse, zur Beiziehung der Strafverfolgungsbehörden – und zum Aufbauen eines Notbetriebs, um rasch wieder wirtschaftlich geschäften zu können. Denn vom Produktionsunterbruch könnte laut Mayencourt die grösste Gefahr ausgehen: «Die Angestellten sollen arbeiten, Löhne müssen bezahlt werden. Und Kunden erwarten fristgerechte Lieferung.» Falls aber das Unternehmen wegen der IT-Probleme nicht oder nur eingeschränkt liefern kann und dies womöglich über einen längeren Zeitraum, kann das «rasch die Existenz bedrohen», wie Mayencourt sagt: «Das kann einen Betrieb Kopf und Kragen kosten.»

Die weiteren Antworten auf einen Fragenkatalog an Huber+Suhner fallen knapp aus. Firmensprecher Köppe schreibt: «Wir stehen mitten in der Arbeit und werden davon absehen, ungesicherte Informationen zu kommunizieren.» Er bestätigt aber, dass die Produktion nach wie vor unterbrochen sei, und zwar «an allen Standorten von Huber+Suhner». Und weiter: «Die von einem Produktionsunterbruch betroffenen Mitarbeiter erscheinen zurzeit nicht zur Arbeit. In den Verwaltungsbereichen wird weltweit gearbeitet, wenn auch mit gewissen Einschränkungen.»

Vergleich mit Attacke auf den Bahnbauer Stadler

Zum betriebswirtschaftlichen Schaden gesellt sich laut Mayencourt der Schaden an der IT-Infrastruktur: «Den infizierten Geräten kann man nicht mehr trauen. Eigentlich müsste man alles ersetzen.» Ein weiterer Punkt sei der Reputationsschaden. Dies, weil sich die unbekannten Täter erfolgreich Zugang verschafft hätten zu den IT-Systemen. Mayencourt sagt: «Hätte Huber+Suhner eine super IT-Sicherheitsarchitektur, hätte diese den Cyberangriff abgewehrt. Wäre die Architektur wenigstens sehr gut, hätte zumindest der Schaden eingedämmt und das totale Herunterfahren der Systeme verhindert werden können.» Dass der Konzern jedoch als Folge der Attacke alle Arbeitsstationen und die gesamte Produktion global lahmgelegt hat, zeigt für Mayencourt: «Bei Huber+Suhners IT-Sicherheitsarchitektur liegt wohl ganz vieles im Argen.»

IT-Sicherheitsexperte Nicolas Mayencourt. Bild: PD

Der Angriff mit Schadsoftware erinnert an die Cyberattacke auf den Schienenfahrzeugbauer Stadler vergangenen Mai. Damals stahlen die unbekannten Täter Daten und drohten mit deren Veröffentlichung, sollte Stadler nicht sechs Millionen Dollar in Bitcoin zahlen. Stadler gab dem Erpressungsversuch nicht nach, worauf die Täter zwei Mal Daten im Darknet veröffentlichten, die allerdings alt waren, was Stadler folglich nicht schadete. Der anonyme Twitter-Account, der die Datenpublikationen jeweils verkündete, ist mittlerweile gesperrt.

Auch im Fall Huber+Suhners geht Mayencourt davon aus, dass es sich um «Cybercrime as usual» handelt, sprich, um einen Erpressungsversuch: «Die Täter wollen Geld.» Auf die Frage, ob bei Huber+Suhner eine erpresserische Geldforderung eingegangen sei, gibt Firmensprecher Köppe keine Antwort. Auch nicht auf die Fragen, inwieweit Huber+Suhners Lieferfähigkeit beeinträchtigt ist und was der Produktionsunterbruch für Kunden und Zulieferer bedeutet. Auf Fragen über mutmassliche Defizite in der IT-Sicherheitsarchitektur und ob Huber+Suhner daran arbeitet, einen Notbetrieb zum Wiederanlaufen der Produktion einzurichten, geht Köppe ebenso wenig ein.

Stadler-Chef Peter Spuhler sagte im August anlässlich der Vorlage des Semesterberichts, er erachte den Fall des Cyberangriffs auf sein Unternehmen als erledigt im Sinne von: Er glaube nicht, dass die Erpresser nochmals vorstellig würden und etwas gegen Stadler in der Hand hätten. Die Ermittlungen der Staatsanwaltschaft Thurgau dauern dagegen an. «Die Strafuntersuchung im Fall Stadler ist pendent», sagt Behördensprecher Marco Breu. Ermittelt wird unter anderem wegen gewerbsmässiger Erpressung. Diese ist ein Offizialdelikt, muss also von Amtes wegen verfolgt werden. Weitere mutmassliche Delikte sind unbefugtes Eindringen in ein Datenverarbeitungssystem, Datenbeschädigung und unbefugte Datenbeschaffung.

Corona begünstigt Internetkriminalität

Im Unterschied zu Huber+Suhner konnte Stadler nach dem Angriff die Produktion der Züge unvermindert aufrechterhalten und auch stets alle Serviceleistungen erbringen. Mayencourt sagt, «Stadler ist höchstwahrscheinlich relativ glimpflich davongekommen». Firmensprecher Fabian Vettori äussert sich dazu nicht. Dass aber bei Huber+Suhner die Produktion unterbrochen ist, zeigt laut Mayencourt: «Die IT-Sicherheitsarchitektur ist zu wenig segmentiert.» Er vergleicht den Idealfall mit dem Schiffbau, wo Schotten, also durchgehende Trennwände, im Fall eines Lecks verhindern, dass der ganze Rumpf mit Wasser vollläuft.

Im Gespräch mit Mayencourt fällt auch das Wort Corona. Als Folge der Pandemie sei die IT noch verwundbarer geworden. Der Experte nennt zwei Beispiele. Zum einen habe Homeoffice zu einem Digitalisierungsschub geführt, der aber «oft nicht sicher genug ist». Mayencourt sagt: «Jeder einzelne Mitarbeitende bietet eine Angriffsfläche, und das hat sich nun potenziert.» Zum andern nennt er das gesteigerte Informationsbedürfnis der Gesellschaft wegen Corona: «Die Leute wollen immer neue Informationen. Das hat es Trickbetrügern erleichtert, zum Beispiel in E-Mails betrügerische Links zu platzieren.» Was tun? Nicolas Mayencourt hat ein einfaches Rezept parat: «Ich kann nur raten, nicht alles aus Neugier anzuklicken.»

Präsent in 80 Ländern

Huber+Suhner mit Hauptsitz in Herisau und Pfäffikon ZH ist in der elektrischen und optischen Verbindungstechnik tätig. Das Unternehmen stellt Kabel, Stecker, Antennen usw. her. Der Konzern hat in Werken und Vertretungen in 80 Ländern 4700 Mitarbeitende. In der Schweiz zählt Huber+Suhner 1250 Angestellte, davon 700 in Herisau und 550 in Pfäffikon. In den ersten neun Monaten 2020 betrug der Umsatz 563 Millionen Franken und der Auftragseingang 571 Millionen Franken. *(T. G.)*

Schutzmasken, Fresspäckli, Fertigmenus

Der Tübacher Automatenfirma Leomat scheinen die Ideen nicht auszugehen.

Die 60 Mitarbeitenden der Tübacher Firma Leomat und Geschäftsführer Daniel Büchel tüfteln stets an Neuheiten. «Wir haben schon etwas den Ruf, immer auf der Suche nach Innovationen zu sein», bestätigt Büchel. Jüngster Streich: Leomat hat einen kompakten Automaten namens «Safety Point» entwickelt. Dieser wird ausschliesslich mit Hygiene- und Desinfektionsprodukten bestückt, also mit Schutzmasken, Desinfektionsmittel und Handschuhen. Bezahlt wird per Twint.

Gedacht ist der Automat für Firmen, Restaurants, Vereine oder Sport- und Freizeitanlagen. Wichtig ist laut Büchel: «Es geht um Verfügbarkeit und Hygiene.» Deshalb sind beispielsweise die Schutzmasken aus dem Automaten einzeln in Karton verpackt. So sind sie sauber und können auch mitgenommen werden. «Wenn Sie dagegen eine Schachtel mit 50 Masken aufstellen und jeder greift rein, ist bald die ganze Packung verseucht», sagt Büchel.

Ebenso wichtig ist für Büchel, dass alle Artikel, mit denen er die Automaten bestückt, aus Schweizer Produktion stammen, so etwa die Masken des Labels «Masktogo», ein Projekt von Schweizer Firmen und Stiftungen, die lokal für den Schweizer Markt produzieren. In der Regel betreibt Leomat die Automaten. Aber es ist auch möglich, einen Automaten zu kaufen und nach eigenem Gusto zu bestücken. Büchel hat bereits zehn Automaten im Einsatz.

Leomat-Geschäftsführer Daniel Büchel und der neue Automat «Safety Point» für Schutzmasken und Co. Bild: Frosan von Gunten/PD

Im Frühling 2020 hat Leomat mit einem anderen Automaten Aufsehen erregt. Lanciert wurde damals die «Genussbox», ein Verpflegungsautomat in einem Container für Baustellen. Wie Büchel sagt, laufen diese Automaten gut, doch nicht die Container, denn: «Die Baufirmen stellen die Automaten in ihre eigenen Container.» Dennoch ist Büchel froh über die «Genussbox», denn «auf den Baustellen wird gearbeitet, die meisten anderen Angestellten sind ja im Homeoffice».

Doch auch daraus ergeben sich neue Geschäftschancen. Wie Büchel sagt, hat er zwei Projekte in der Pipeline, die demnächst auf den Markt kommen sollen. Zum einen will Leomat Verpflegungspakete schnüren und an Leute schicken, die zu Hause arbeiten. Zum anderen wird es Fertigmenus «in hochwertiger Qualität» aus dem Automaten geben. Gedacht sind diese Menus in erster Linie für Leute, die an ihrem Arbeitsplatz sind, die aber Schwierigkeiten haben, sich zu verpflegen, etwa weil ihre Kantine oder Restaurants geschlossen sind. Bei den Fertigmenus soll es zwei Linien geben, die eine für die Mikrowelle und die andere für die Zubereitung in einer speziellen Maschine des Amriswiler Geräteherstellers Eugster Frismag.

Thomas Griesser Kym