Datum: 27.07.2022

NEBELSPALTER

Online-Ausgabe

Nebelspalter
8002 Zürich
044 242 87 87
https://nebelspalter.ch/

Medienart: Internet
Medientyp: Publikumszeitschriften
UUpM: 6'500

Web Ansicht

Auftrag: 3007101
Themen-Nr.: 014.222

Referenz: 85055788
Ausschnitt Seite: 1/3

Wirtschaftsschutz

Wenn plötzlich die Millionenforderung eintrifft

27. Juli 2022, Dominik Feusi

Auch mittlere und kleine Unternehmen sind von Datendiebstahl und Erpressung bedroht, und das nicht nur im Internet. Ein früherer Kriminalpolizist bereitet Firmen und ihre Mitarbeiter auf die vielfältigen Gefahren vor – und trainiert sie für den Ernstfall.

Der Auftritt wirkt echt. Mitten im Morgenrapport des Landspitals stürmt der Chefarzt im weissen Kittel in das Sitzungszimmer. Er hat eine Mail erhalten. «Organisieren sie innert drei Tagen fünf Millionen Franken, oder ich werde sie zerstören. Was ist ein Menschenleben wert? Ich habe andere Möglichkeiten, als sie denken», heisst es darin.

Was wichtig ist:

Menschen, Know-how, Kapital und Daten sind nicht nur im Internet Gefahren ausgesetzt.

Unternehmen müssen sich ganzheitlich schützen und ihr Personal sensibilisieren.

Und wenn etwas passiert, müssen sie richtig reagieren.

Die neun Teilnehmer des Nachdiplomkurses «Business Protection» der privaten Hochschule für Wirtschaft Zürich (HWZ), bekommen eine halbe Stunde Zeit, das Problem zu analysieren, die Lage zu beurteilen, Sofortmassnahmen zu treffen und sich zu organisieren. Wer muss eingeschaltet und informiert werden? Wie muss sich das Spital schützen? Und wie wird der Vorfall intern und extern kommuniziert?

Gespielt wurde der Chefarzt von Chris Eckert, während dreissig Jahren Kriminalist, zuerst bei der Kantonspolizei Zürich, später bei der Bundeskriminalpolizei. Er berät und trainiert Unternehmen in Sicherheitsfragen und er leitet den Nachdiplomkurs der HWZ (Link).

Faktor Mensch

«Von Risiken im Internet haben mittlerweile die meisten Unternehmen gehört», sagt Eckert. «Doch die Schwachstelle ist in 85 Prozent der Fälle nicht die Technik, sondern der Mensch.» «Human Hacking», nennt Eckert das. Wer seine Organisation, deren Menschen, die Infrastruktur und die Informationen schützen wolle, müsse deshalb mit den Menschen arbeiten.

«Wir alle kennen das Phishing-Mail, mit dem Daten abgegriffen werden sollen», sagt Eckert. «Aber wer die richtigen Informationen hat, kann zum Beispiel der Buchhaltung am Freitag um vier Uhr eine fingierte Mail vom CEO schicken, mit der Anweisung, 50’000 Franken an ein Konto der Angreifer zu überweisen.» Dann müssten die Zahlungsprozesse in der Firma geregelt, Unterschriftenregelungen bekannt und die Mitarbeiter auf Gefahren sensibilisiert sein. Das Gleiche gilt zur Verhinderung von Industriespionage: Wer in ein Unternehmen eindringen will, benötigt dafür die richtigen Informationen.

Physisch eindringen ist gar nicht so schwer

Und wie kommen Verbrecher an diese Daten? Eckert kennt zahlreiche Schwachstellen. «Da ist das manipulative Gespräch mit der Empfangsdame, der Servicetechniker, der ganz dringend in den IT-Raum oder das Sitzungszimmer der Geschäftsleitung muss, oder der Lieferant, der dem CEO einen Brief überreichen muss.» Auch eine Putzequipe mit ihrem unpersönlichen Badge komme überall hin.

Eckert und sein Team beüben ihre Kunden auch. Er versucht dann, dem CEO eine Visitenkarte auf seinem Schreibtisch zu deponieren, oder einen Aktenordner mitgehen zu lassen. In den allermeisten Fällen klappt das. Oder er fotografiert Notizen, zum Beispiel mit Passwörtern, welche der Geschäftsführer auf dem Pult liegen gelassen hat. Oder er greift im Abfallkübel nach dem letzten Strategiepapier des Verwaltungsrates.

Der «Rauchertrick»

Eine andere Variante des sogenannten «Social Engineering» ist der «Rauchertrick», vorwiegend bei grösseren Firmen. Eckert findet heraus, wann und wo die Raucher ausserhalb des Gebäudes eine Rauchpause machen und wie sie aussehen. «Ich stelle mich dann in ähnlicher Kleidung dazu, und nach der Pause komme ich ohne Badge ins Gebäude und meist auch noch in die Teppichetage.» Ein einziges Mal habe ihn eine Mitarbeiterin mit hochrotem Kopf angesprochen und gefragt, wer er sei. «Sie hatte Angst, ich würde mich bei ihrem Chef für die Frage beschweren – dabei hat sie genau richtig gehandelt.»

Das Problem: Geschäftsleitungen und Verwaltungsräte hätten das Thema Sicherheit meist nicht zuoberst auf der Agenda – und wenn, dann höchstens Cybersicherheit. Eine umfassende Unternehmenssicherheit sei komplex und koste nur, so ist oft die Haltung. Es komme vor, dass die IT-Sicherheit dem Haustechniker überlassen werde, erzählt Eckert. Oder die Informatik werde an eine externe Firma vergeben, und man hoffe, dass dann alles in Ordnung sei. « Das reicht heute nicht mehr. Eine integrale Sicherheit muss als Prozess gesehen werden, nicht als ein einmalig erworbenes Produkt» sagt Eckert. Alle Arten von Angriffsmöglichkeiten erkennen sowie die richtigen Gegen- und Abwehrmassnahmen implementieren, das sei die Lösung.

Die Wanze auf dem Stick

Mit den Nachdiplomstudenten trainiert Eckert nicht nur die Vorbeugung von «Social Engineering» und «Human Hacking», sondern auch, was zu tun ist, wenn es trotzdem passiert. Bei der Bedrohung des Landspitals haben die Kursteilnehmer mittlerweile eine Krisenorganisation hochgezogen. Die Zugänge zum Spital werden überwacht. Als ein Kurier ein Päckchen für den Krisenstab bringt, ahnen die Kursteilnehmer, dass es eine Nachricht des Erpressers sein könnte. Sie überlassen das Öffnen einem Spezialisten der Polizei.

Was sie nicht gemerkt haben: Der Kurier legt auch noch einen USB-Stick in das Sitzungszimmer. Der hat ein hochsensibles Mikrofon und nimmt die Gespräche des Krisenstabes auf. Fünf Tage lang.

Datum: 27.07.2022

NEBELSPALTER

Online-Ausgabe

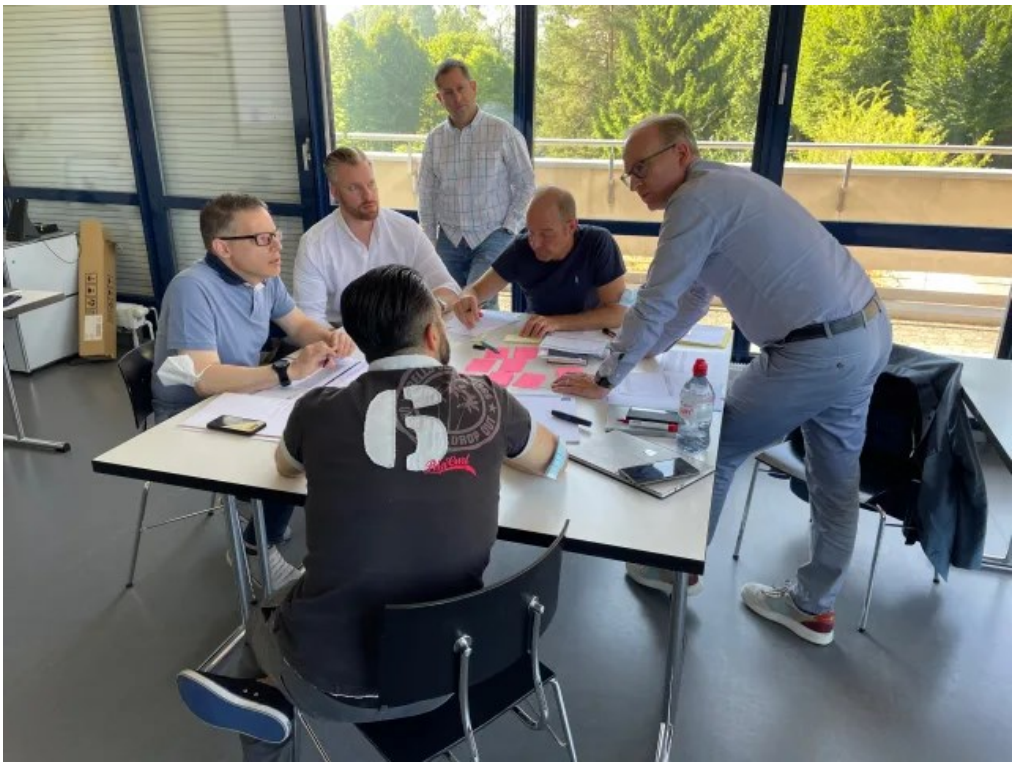
Nebelspalter
8002 Zürich
044 242 87 87
https://nebelspalter.ch/

Medienart: Internet
Medientyp: Publikumszeitschriften
UUpM: 6'500

Web Ansicht

Auftrag: 3007101
Themen-Nr.: 014.222

Referenz: 85055788
Ausschnitt Seite: 3/3



Nachdiplomstudenten der HWZ üben den Ernstfall. (Bild: Dominik Feusi)