Ihre E-Mails sollte man ignorieren

Betrug im Internet Mails sind ein grosses Einfallstor für Datenklau und Erpressung. Eine kleine Berner Firma trainiert die Angestellten von Konzernen mit gefälschten Nachrichten.

Adrian Hopf-Sulc

Sie verschicken jährlich 700'000 Mails: Marcel Oberli (links) und Markus Helfer, Inhaber der Berner Advact AG. Foto: Adrian Moser

«Dringende Gewinnbenachrichtigung» oder «Letzte Mahnung» heisst es manchmal in den Betreffzeilen. Wer nicht völlig neu ist im Internet, wird in solchen E-Mails weder auf einen Link klicken noch den Anhang öffnen.

Doch was ist, wenn die Krankenkasse von einer Ärztin eine angebliche Rechnung im Mail-Anhang erhält – sollen die Angestellten des Kundendienstes diesen öffnen oder die Nachricht löschen? Was macht der Mitarbeiter einer Bank, der ein Mail mit einer angeblichen Sprachnachricht einer Schweizer Handynummer erhält?

«E-Mail ist für Cyberkriminelle der einfachste und billigste Weg, in eine Firma einzudringen», sagt Marcel Oberli. Er ist Mitgründer der Berner Firma Advact, die Unternehmen in Sachen Cybersicherheit berät. Zwar könnten sich Hacker auch Zugang zu den Firmencomputern verschaffen, indem sie nach Sicherheitslücken im System suchten. Doch das benötige viel Know-how und viel Zeit.

E-Mails können hingegen beliebig breit gestreut werden. Irgendjemand wird schon anbeissen. Um das zu verhindern, verfassen die Mitarbeiter von Advact teilweise selber Betrugsmails – um die Empfänger entsprechend zu schulen.

Ein Albtraum für jede Firma

Die echten Betrüger locken ihre Opfer auf gefälschte Log-in-Seiten für soziale Medien oder für Firmensysteme, um ihnen Passwörter zu entlocken. Dann handelt es sich um sogenanntes Phishing.

Oder sie versuchen, auf dem Computer der Empfänger schädliche Software zu installieren. Oft handelt es sich um Verschlüsselungstrojaner: Diese blockieren sämtliche Daten auf dem Computer und geben sie erst wieder gegen ein Lösegeld frei. Das kann die gesamten Daten eines Unternehmens betreffen – Kundenlisten, Datenbanken, aktuelle Bestellungen. Ein Albtraum für jeden Betrieb.

Solche Software müsse nicht einmal selbst programmiert werden, sondern lasse sich im Internet erwerben, sagt Oberli. Entsprechend würden viele Cyberkriminelle ihr Glück versuchen und mehr oder weniger raffiniert formulierte Mails mit solchen Trojanern im Anhang verschicken.

Gerne werden kleine und mittlere Unternehmen erpresst: «Die KMU sind meist schlecht geschützt, und die Erpresser können auch dort 10'000 oder 15'000 Franken verlangen, um die Daten wieder freizugeben», so Oberli. Doch auch grosse Unternehmen stehen im Fokus der Täter – und rüsten entsprechend auf. Oberlis Firma Advact zählt unter anderem die Post und die SBB zu ihren Kunden, ebenso mehrere Schweizer Krankenkassen und Kantonsverwaltungen.

Gute E-Mail-Filter fangen laut Oberli zwar über 95 Prozent der betrügerischen Mails ab. Bei den restlichen 5 Prozent bleibt das Risiko des menschlichen Fehlers. «Selbst geschulte Mitarbeiter erkennen nicht alle solchen E-Mails.» Deshalb haben die Sicherheitsspezialisten vor fünf Jahren den «Phishing-Service» ins Leben gerufen, bei dem sie ihren Kunden vermeintliche Betrugsmails zuschicken – mit dem Ziel, dass diese lernen, solche zu erkennen.

Die Absender der Betrugsmails sitzen oft in Osteuropa und sind juristisch kaum fassbar.

Namhafte Kunden

Damit die falschen Phishing- und Trojaner-Mails nicht gleich auffallen, werden sie allen Angestellten einer Firma über ein ganzes Jahr oder länger verstreut zugeschickt. Wer sie anklickt, fängt sich keinen Virus ein, aber erfährt, dass er darauf reingefallen ist. «So lernen die Angestellten viel besser, solche Mails zu erkennen, als in einer einmaligen Onlineschulung», sagt Oberli. Das Programm, das die Mails verschickt, misst, wie viele Prozent der vermeintlich gefährlichen Links angeklickt werden. Je nachdem, ob jemand oft oder selten auf die Mails hereinfällt, erhält er einfacher oder schwieriger zu erkennende Betrugsmails.

Namentlich lassen unter anderem Securitas, die Gebäudeversicherung Bern, Helsana, KPT und Visana ihren Mitarbeitenden solche Mails zuschicken, andere grosse Unternehmen wollen nicht genannt werden.

Advact hat auch das VBS und die Parlamentsdienste des Bundes als Kunden gewonnen. Die Bundesstellen rüsten sich nicht nur aus blosser Vorsicht gegen Cyberkriminalität: Vor einigen Jahren wurden Mitarbeitende des Aussendepartements mit individuell erstellten Phishing-Mails geködert, und bei der mit dem Verteidigungsdepartement verbandelten Ruag kam es 2016 zu einem grösseren Datendiebstahl.

Insgesamt verschickt Advact pro Jahr 700'000 bis 800'000 vermeintliche Phishing-Mails. Im Verlauf des Jahres will die Firma das Mail-Trainingsprogramm kostenlos für Privatpersonen und Kleinstunternehmen öffnen.

Heute erzielt das von Marcel Oberli und Markus Helfer geführte Unternehmen über die Hälfte des Umsatzes mit ihrem Phishing-Service. Dies auch dank eines neuen Service, mit dem die Kunden ein verdächtiges Mail überprüfen lassen können – etwa besagte angebliche Arztrechnung.

Mensch statt Maschine

Über einen Knopf im E-Mail-Programm kann ein solches Mail zu Advact verschoben werden. Ein Analysetool des ETH-Spin-off-Unternehmens Xorlab prüft die Mails auf bekannte Text- und Codezeilen und auf verdächtige Absender. Wenn das Mail nicht bereits hier als schädlich erkannt wird, prüfen es noch die neun Mitarbeiter von Advact.

Dafür sind sie in Schichten eingeteilt, in denen sie gemeldete Mails abarbeiten müssen. Dabei bekommen sie allerhand zu sehen: zwielichtige Werbeanzeigen, oft mit nackten Frauen, verschiedenste Betrugsmaschen und diverse Viren und Trojaner. Pro Monat melden die Advact-Kunden durchschnittlich 10'000 E-Mails zur Analyse. Gut 1500 davon sind Phishing- oder andere Betrugsmails und weitere 20 solche mit funktionierender Schadsoftware im Anhang. Bei einem Drittel handelt es sich um unerwünschte, aber harmlose Spammails und beim Rest um legitime E-Mails – oder um Simulationsmails von Advact selbst.

Dass so Schadsoftware durchschlüpft, ist laut Oberli praktisch ausgeschlossen. Ihm ist ein einziger Fall bekannt, in dem ein betrügerisches Mail für harmlos befunden wurde: eine echte Rechnung, die von Kriminellen jedoch abgefangen und mit einer falschen IBAN versehen worden war. Der Fehler flog dann in der Buchhaltung des Unternehmens auf, bevor das Geld auf das Konto des Betrügers überwiesen worden war.

Wäre es nicht besser, das E-Mail-Problem an der Wurzel zu bekämpfen, statt die Mails mit ausgeklügelten Systemen herauszufiltern? Oberli winkt ab. Man sehe in den Betrugsmails zwar die Serveradressen der Versender. «Aber wir gehen dem nicht nach.» Die kriminellen Netzwerke, oft in Osteuropa und Russland, sind juristisch kaum fassbar. Absender und Betrugsmaschen würden laufend ändern – «wie die Varianten des Coronavirus». Entdecke man eine neue, würden die Server mit einem Update «geboostert» und könnten dann künftig auch diese herausfiltern. Bis der neuste Trojaner auftaucht und unvorsichtige Angestellte zum Klick verleitet.

Falsche Mails von DHL, Post und Polizei

Frau G. erhält ein E-Mail von der Schweizerischen Post: Ein Paket hänge beim Zoll fest. Es seien noch 2.99 Franken Gebühren fällig, sonst werde das Päckli aus Deutschland nicht zugestellt. Sie erwartet tatsächlich ein Paket aus Deutschland. So klickt sie auf den Link, kommt auf eine seriös aussehende Website mit Post-Logo – und bezahlt den Betrag per Kreditkarte. Bald bekommt Frau G. aber Zweifel, ob sie nicht einem Betrug aufgesessen ist. Eine halbe Stunde später ruft sie bei der Kreditkartenfirma an und lässt ihre Karte sperren. Sie hat Glück: Es wurde noch kein Geld abgebucht.

Natürlich stammt das Mail nicht von der Post. Genauso wie angebliche Mails von DHL, der Kantonspolizei oder der Steuerverwaltung stammt es von Cyberkriminellen.

Was kann man gegen solche Mails tun? Nicht viel, sagt der Berner IT-Unternehmer Marcel Oberli: «Aus diesen Adresslisten kommen Sie nicht mehr raus» – selbst wenn es im Mail einen angeblichen «Abmelden»-Knopf gibt. Man ist auf die Spam-Filter seines Mail-Anbieters angewiesen – oder legt sich eine neue Adresse zu.

Wie erkennt man, ob das Mail echt ist? Ein Blick auf die Internetadresse hinter einem Link verrät, wohin dieser wirklich führt – auf post.ch/xyz oder auf eine nachgeahmte Seite wie etwa post.ch.website.com/xyz (dafür den Link nicht anklicken, sondern mit der Maus nur darüberfahren oder auf dem Smartphone lange draufbleiben).

Im Zweifelsfall kann man sich beim betreffenden Unternehmen telefonisch erkundigen, ob der Sachverhalt im Mail stimmt. Das Nationale Zentrum für Cybersicherheit veröffentlicht auf seiner Website eine Liste von E-Mail-Betrugsversuchen (ncsc.admin.ch).

Wer auf einer gefälschten Seite sein Passwort angegeben hat, sollte dies auf der echten Seite umgehend ändern. Damit Internetbetrügern nur ein Schlüssel und nicht gleich ein ganzer Schlüsselbund in die Hände fällt: nie das gleiche Passwort für mehrere Internetseiten verwenden.

Um im Fall eines Virenbefalls oder eines Verschlüsselungstrojaners den Schaden gering zu halten, empfiehlt Marcel Oberli, alle eigenen Daten regelmässig zu sichern – sei es bei einem Anbieter in der Cloud oder auf einer externen Festplatte, die dann vom Computer abgehängt wird. *(sul)*