Die Betrugsversuche von Hackern werden immer raffinierter.

DER TEUFEL LIEGT IM DETAIL

DER PHISHING-FALLE ENTGEHEN

von Andreas Wisler

«Bitte Kontodaten eingeben.» So kennen wir Phishing-E-Mails schon seit einiger Zeit. Die Faktoren schlechte Rechtschreibung, verdächtige Absender und unpersönliche Anreden sind mittlerweile bekannt und überzeugen fast niemanden mehr. Jedoch ist auch bekannt, dass die Gauner des Internets uns meist einen Schritt voraus sind. Nicht nur beim Erschaffen von Viren, welche nicht erkannt werden, sondern auch von immer professionelleren Phishing-E-Mails. Plötzlich enthält ein E-Mail eine persönliche Anrede, korrektes Deutsch oder die persönliche Wohnadresse. Doch woher kommen all diese persönlichen Informationen?

Das Zauberwort lautet «Data Breaches». Beinahe monatlich wird über ein Unternehmen berichtet, dessen Daten gestohlen wurden. Diese Daten können bequem im Online-Shop des Darknets gekauft und daraus ein sehr persönliches Phishing-E-Mail erstellt werden. Doch wie kann nun eine solche Nachricht zweifelsfrei erkannt werden? Eine allgemeine Regel gibt es nicht (mehr). Jedoch helfen immer noch einige Anhaltspunkte.

DER ABSENDER

Wenn vom Chef eine E-Mail kommt, muss schnell reagiert werden. Genau dies macht sich ein Angreifer zunutze. Die Autorität des Vorgesetzten kombiniert mit einem E-Mail, aus welchem Zeitdruck hervorgeht, ist die perfekte Falle. Vermutlich ist dies jedem schon mal passiert, dass er in diesem Fall zu schnell gedrückt hat. Durch eine saubere Vorbereitung weiss der Hacker genau, wie die Hierarchie in der Firma aussieht. Das Organigramm auf der Firmen-Homepage oder die Einträge auf Xing/LinkedIn helfen dabei ungemein. Genaues Hinschauen bei der Absenderadresse ist notwendig. Nur ein Buchstabe ausgewechselt und schon ist der Absender ein vollkommen anderer. Auf Smartphones ist es noch schwieriger, den Unterschied zu erkennen. Dort wird auf den ersten Blick nur angezeigt, was der Angreifer sehen lassen will: Name und Betreff. Erst ein Klick auf «View Details» zeigt, um welche Adresse es sich wirklich handelt.

DER INHALT

Der Inhalt bietet ebenfalls ein wichtiges Indiz. Wenn der interne Ablauf für eine Zahlung klar geregelt ist und plötzlich der Chef via E-Mail verlangt, eine grosse Summe zu überweisen, ist das verdächtig. Es gilt, auf Formulierungen, Schreibstil oder Grussworte zu achten. Wenn zum Beispiel der Lieferant immer mit «Gruss Max» das E-Mail beendet und nun steht «Freundliche Grüsse Max». Das sind Details, welche von jemandem, der noch nie E-Mails von dieser Person erhalten hat, nicht erkannt werden. Aber wenn einem die andere Person bekannt ist, wird man stutzig. Und auf dieses Gefühl sollte gehört werden. Es bewahrt einem möglicherweise vor grossem Schaden.

DIE FORMATIERUNG

Auch die Schriftart ist ein Detail, die eine Person oder ein Geschäft ausmacht. Es gibt wenig Gründe, weshalb sich die Schriftart verändert. Sieht das E-Mail plötzlich anders aus, ist wieder Vorsicht geboten.

TECHNISCHE FALLEN

Aber was, wenn alle oben erwähnten Tests positiv, im Sinne der Gültigkeit, ausfallen und im empfangenen E-Mail ein Link oder eine Datei vorhanden ist? Dazu gibt es einige Tricks, die auf technischer und sozialer Ebene angewendet werden können.

Anhänge sind immer ein sehr schwieriges Thema. Am sichersten wäre es, wenn gar keine Dateien via E-Mails geöffnet werden. Denn mittlerweile wurde schon in vielen Arten von Dateien Viren oder Trojanische Pferde (ein in einer anderen Datei versteckter Schädling) entdeckt. Aber das ist im Geschäftlichen wie im Privaten keine akzeptable Lösung. Die Einschränkung ist zu gross. Somit muss von Dateityp zu Dateityp unterschieden werden. Als relativ sicher gilt immer noch ein PDF. Der PDF-Reader muss jedoch aktuell sein. Besser noch, ein «dummes» PDF-Programm verwenden, das PDFs anzeigt, aber keinen Code ausführt. Aber auch in einfachen Bildern ist es möglich, Malware zu verstecken. Hier gilt ebenfalls: Bild anzeigen ja, Code ausführen nein. Ganz klare Tabus sind Office-Dateien mit Makros, welche mit den Endungen .xlsm, .xltm oder .docm erkannt werden können. Die grösste Sicherheit bietet eine sichere Web-Datenablage. Diese kann bei Projekten mit internen oder externen Partnern gebraucht werden. Damit kann auf den Austausch von Daten via E-Mail verzichtet werden.

Um persönliche Daten zu schützen, gilt es, im Internet achtsam zu sein.

Links in E-Mails werden häufig sehr kritisch betrachtet. In vielen Fällen werden solche E-Mails sofort gelöscht. Dies ist aber gar nicht nötig. Das Zauberwort hier heisst «Mouse-Over». Einfach mit der Maus über den Link fahren und wenige Augenblicke warten, schon erscheint ein Popup-Fenster, in welchem die wirkliche Ziel-Adresse angezeigt wird. In den meisten Anwendungen ist diese Funktion enthalten. Falls das nicht der Fall ist, gibt es immer noch die Möglichkeit, einen Rechtsklick auf den Link auszuführen und dann die Link-Adresse zu kopieren. Auch hier ist uns die dunkle Seite des Netzes aber wieder einen Schritt voraus. In äusserst seltenen Fällen verwenden Hacker andere Alphabete mit denselben Buchstaben. Somit sieht der Link im Popup-Fenster richtig aus, jedoch werden andere Zielserver angesprochen. Deshalb ist es am sichersten, wenn der Link manuell in der Browser-Adresszeile eingegeben wird.

DER SOZIALE ASPEKT

Eine persönliche Rückfrage ist immer noch die beste Methode, um die Echtheit einer E-Mail zu prüfen. Aber auch hier gibt es «do's and dont's». Niemals darf für die Überprüfung auf die E-Mail geantwortet werden. Denn wenn der Angreifer alles richtig gemacht hat, bekommt er diese Antwort und teilt dem Opfer mit, dass alles in Ordnung ist. Am besten wird zum Telefon gegriffen. Falls es doch ein E-Mail sein muss, sollte ein neues erstellt und die E-Mail-Adresse des Empfängers manuell eingetragen werden. ●

MERKPUNKTE:

- Lieber einmal zu viel nachfragen. Wer schon einmal eine Verschlüsslungs-Malware (Ransomware) auf dem Computer hatte, weiss, wie zeitintensiv es ist, diese wieder zu entfernen.
- E-Mail-Adressen oder Links von Hand eingeben. Beim Kopieren werden alle Teile mitgenommen, welche eventuell nicht gewünscht sind.
- Auf Details achten. Immer die komplette E-Mail-Adresse lesen.
- Bei Verdacht auf das Bauchgefühl hören.

ANDREAS WISLER

ist Inhaber und Senior Security Auditor bei der goSecurity GmbH.

www.gosecurity.ch