LASSEN SIE SICH NICHT PHISHEN

«Bite konto daten 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 Internet-Gauner oft 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 Informationen über Sie?

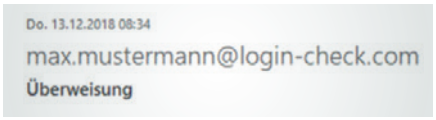
von Andreas Wisler

Der Grund sind so genannte «Data Breaches». Beinahe wöchentlich wird über ein Unternehmen berichtet, dessen Kunden-Daten gestohlen wurden. Diese Daten können danach bequem im Online Shop im Darknet 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 gibt es immer noch einige Anhaltspunkte, die Ihnen helfen können.

DER TEUFEL LIEGT IM DETAIL: DER ABSENDER

Wenn vom Chef eine E-Mail kommt, dann muss schnell reagiert werden. Oft so schnell, wie wenn der Chef neben Ihnen steht. Genau dies macht sich ein Angreifer zunutze. Die Autorität des Vorgesetzten, kombiniert mit einem E-Mail, aus welchem Zeitdruck hervorgeht, ist eine 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 zudem genau, wie die Hierarchie in der Firma aussieht. Das Organigramm auf der Firmen-Homepage oder die Einträge auf Xing/Linkedin helfen dabei ungemein.

Nehmen wir an, Sie erhalten eine Nachricht Ihres Chefs. In unserem Beispiel wäre das Herr Max Mustermann von der Firma Login-Check. Die offizielle Webseite ist unter https://www.login-check.com erreichbar.



1. Version

2. Version

Erkennen Sie den Unterschied? Nur schon ein Buchstabe ausgewechselt, bei unserem Beispiel sind es drei, und schon ist der Absender ein vollkommen Anderer. Deshalb ist genaues Hinschauen notwendig. Auf Smartphones ist es noch schwieriger den Unterschied zu erkennen. Dort wird auf den ersten Blick nur angezeigt, was der Angreifer Sie 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 Ihr Chef via E-Mail verlangt, eine grosse Summe zu überweisen, ist das verdächtig. Mit Details beziehe ich mich hier auf Formulierungen, Schreibstiel, Grussworte. Wenn zum Beispiel der Lieferant immer mit «Gruss Max» das E-Mail beendet und nun steht «Freundliche Grüsse Max». Das sind Details, welche von jemanden, der noch nie

E-Mails von dieser Person erhalten hat, nicht erkannt werden. Aber wenn Sie die andere Person kennen, bekommen Sie ein seltsames Gefühl, da stimmt doch etwas nicht. Und auf dieses Gefühl sollte gehört werden. Es bewahrt möglicherweise vor grossem Schaden.

DIE FORMATIERUNG

Vielleicht haben Sie eine besondere Schriftart, die Sie mögen und für Ihre E-Mails verwenden. Auch dies ist wiederum ein Detail, die eine Person oder ein Geschäft ausmachen. Es gibt wenig Gründe weshalb die Schriftart sich plötzlich verändert. Sieht das E-Mail anders aus, ist wieder Vorsicht angezeigt.

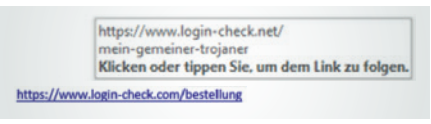
PRÜFEN SIE: TECHNISCH

Aber was, wenn man sich wirklich nicht sicher sein kann. 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, welche Sie anwenden können.

Anhänge sind immer ein heikles Thema. Am sichersten wäre es, wenn gar keine Dateien, welche Sie über ein E-Mail erhalten haben, geöffnet werden. Denn mittlerweile wurde schon in vielen Arten von Dateien Viren oder trojanische Pferde (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, wie mit dieser umgegangen werden kann. Als relativ sicher gilt immer noch ein PDF. Aber auch hier gilt wieder: Der PDF-Reader muss aktuell sein. Oder besser noch, ein «dummes» PDF-Programm, 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, .docm usw. erkannt werden können.

Am besten ist es, eine sichere Web-Datenablage einzurichten. Diese kann bei Projekten mit internen oder externen Partnern gebraucht werden. Damit kann auf den Austausch von Daten via E-Mail verzichtet werden.

Bei Interviews, welche wir mit den Mitarbeitenden während eines Audits durchführen, zeigt sich oft die Tendenz, dass Links in E-Mails sehr kritisch betrachtet werden. In vielen Fällen werden solche E-Mails sofort gelöscht. Ich will Ihnen aber einen einfachen und schnellen Weg aufzeigen, wie Sie einen solchen kontrollieren können. Die Funktion dazu heisst «Mouse-Over». Einfach mit der Maus über den Link fahren und wenige Augenblicke später 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 uns aber wieder einen Schritt voraus. In äusserst seltenen Fällen verwenden Hacker andere Alphabete mit denselben Buchstaben (zum Beispiel das russische Alphabet). Somit sieht der Link im Popup-Fenster richtig aus, jedoch werden andere Server im Internet aufgerufen. Deshalb ist es am sichersten, wenn der Link manuell in der Browser-Adresszeile eingeben wird.

FRAGEN

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 Ihnen mit, dass alles in Ordnung ist. Am besten wird zum Telefon gegriffen. Falls es doch ein E-Mail sein muss, sollte ein neues erstellt werden und die E-Mail-Adresse des Empfängers manuell eingetragen werden.

MERKEN SIE SICH:

- dass Sie 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.
- dass Sie E-Mail-Adressen oder Links von Hand eingeben. Denn beim Kopieren werden alle Teile mitgenommen, welche eventuell nicht gewünscht sind.
- dass es auf die Details ankommt. Lesen Sie immer die komplette E-Mail-Adresse.
- Hören Sie auf Ihr Bauchgefühl, wenn Sie den Eindruck haben, dass etwas nicht stimmt.

Mit diesen einfachen Kniffs können Sie sich auch in Zukunft vor den Phishern schützen und sich weiterhin unbeschwert im Internet bewegen.

KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen
Telefon +41 (0)52 511 37 37

info@goSecurity.ch
www.goSecurity.ch