

FAKTOR MENSCH IN DER IT-SICHERHEIT



Phishing: Mit Phishing-Mails (von fishing, engl. für „Angeln“) versuchen Kriminelle immer wieder an die Passwörter der Empfänger zu gelangen.

PHISHING, MALWARE & CO. – SICHERER UMGANG MIT E-MAILS

Sicherheitsbewusstsein als essenzielle Ergänzung zu technischen Schutzmaßnahmen

Firewalls, Anti-Virus-Lösungen, Intrusion Detection- und Prevention-Systeme sowie Backups und regelmäßiges Testen der Datenwiederherstellung sind technische Basis und unverzichtbar zum Schutz vor den tagtäglichen Bedrohungen aus dem Internet.

Der Faktor Mensch, also die Rolle der eigenen Mitarbeiter im Gefahrenszenario, darf jedoch nicht außer Acht gelassen werden. Studien zur Lage der IT-Sicherheit zeigen: Irrtum und Nachlässigkeit eigener Mitarbeiter sind Hauptursache für Schäden in deutschen Unternehmen. Entsprechend sind die häufigsten Ursachen für Datenlecks sogenanntes Social-Engineering, Phishing und Unachtsamkeit. Unter den Infektionswegen für Schadsoftware (Malware) haben E-Mails den Spitzenplatz inne.

Eine Sensibilisierung der Mitarbeiter für die Gefahren aus dem Cyberspace, also die Schaffung sogenannter Security Awareness, ist somit unerlässlich. Privatanwender sind ebenso betroffen.

Malware, gefährliche Anhänge, gefälschte Links – wie schütze ich mich?

E-Mails sind Einfallstor Nummer eins für Viren, Trojaner und andere Schadsoftware. Sie verstecken sich in Dateianhängen oder hinter einem Link und können massiven Schaden anrichten: Angefangen von der allmählichen oder schlagartigen Löschung von Daten über das meist unbemerkte Ausspähen und Versenden von Passwörtern bis zur vollständigen Verschlüsselung aller Daten, einschließlich Lösegeldforderung für deren Freigabe, durch sogenannte Ransomware (Erpressungstrojaner).

Antivirenprogramme vereiteln das Ausführen infizierter Dateien, und mitunter untersuchen und blockieren sie entsprechende E-Mails schon beim Empfang, also noch bevor diese in Ihrem Postfach landen. Aber neue Varianten von Schadsoftware erscheinen quasi im Stundentakt. Es ist daher nur schwer möglich Antivirus-Programme immer topaktuell zu halten. Hier ist deshalb auch der gesunde Menschenverstand gefragt!



Seien Sie aufmerksam im Umgang mit E-Mails: Gefälschte Bestellbestätigungen namhafter Anbieter sind immer häufiger im Umlauf und verleiten dazu Kriminellen unwissentlich Tür und Tor zu Ihren persönlichen Daten zu öffnen.

<http://www.xyz-falsche-domain.com/DGFNX11153/form>

[Ihr monatlicher Rechnungsdownload](#)



Links in der E-Mail auf ihre Validität prüfen: Indem Sie den Mauszeiger darüber bewegen, lassen Sie die tatsächliche Ziel-URL anzeigen.

Der bloße Erhalt einer solchen E-Mail hat noch keine Folgen. Erst durch Öffnen des Anhangs bzw. Anklicken des betreffenden Links wird das Schadprogramm ausgeführt. Grundsatz Nummer 1 lautet daher, niemals Dateianhänge oder Links unbekannter Absender zu öffnen. Aber auch E-Mail-Anhängen bekannter Absender kann nicht bedenkenlos vertraut werden. Viren und Würmer durchsuchen einen befallenen PC nach E-Mail-Adressen

und versenden sich selbst an diese weiter unter der Absenderadresse des eigentlichen Nutzers. So können auch E-Mails, die vermeintlich von Kollegen, Geschäftspartnern oder Freunden stammen, Schadsoftware enthalten. Sollten Sie keinen Dateianhang angefordert haben, vergewissern Sie sich also beim Absender, dass die Nachricht tatsächlich von ihm stammt.

Der Medienbruch nimmt zwar der E-Mail einen Teil ihrer Effizienz und Direktheit; ein kurzer Anruf ist aber immer noch besser, als aufwendig den PC entwanzen zu müssen.

Unternehmen können sich, um den internen E-Mail-Verkehr diesbezüglich abzusichern, sogenannter Authentifizierungstools bedienen. Diese verhindern, dass sich externe Mail-Absender als interne tarnen können.

SECURITY AWARENESS – STÄRKEN SIE DAS IT-SICHERHEITSBEWUSSTSEIN IHRER MITARBEITER



Security Awareness: Mit Schulungen stärken Sie das IT-Sicherheitsbewusstsein Ihrer Mitarbeiter.

Es wurde bereits darauf hingewiesen, dass neben wichtigen technischen Maßnahmen zur IT-Sicherheit vor allem der Faktor Mensch als das schwächste Glied in der gesamten Sicherheitskette eine gewichtige Rolle spielt. Die beste Technik nützt also nichts, wenn statt der Technik der menschliche Benutzer durch sogenannte Social Engineering- oder Human Hacking-Angriffe manipuliert wird. Angreifer finden es offensichtlich einfacher, das Vertrauen von Personen auszunutzen als sich in technisch sichere IT-Systeme zu hacken.

Während im ersten Teil der sichere Umgang mit E-Mails als ein konkreter Baustein zu mehr Sicherheitsbewusstsein im Focus stand, stehen jetzt umfassendere Security Awareness-Schulungen im

Mittelpunkt. Diese Schulungen sollten ein essenzieller Bestandteil Ihrer Gesamtstrategie zur IT-Sicherheit in Ihrem Unternehmen sein.

Social Engineering – Die Kunst der Täuschung

Forscher gehen davon aus, dass ca. 80 Prozent der menschlichen Entscheidungen gefühlsbasiert getroffen werden. Der menschliche Verstand hat demnach in vielen Fällen wenig Mitspracherecht. Und genau diesen Umstand nutzt Social Engineering bzw. Human Hacking aus. Das Angriffsziel sind also nicht die IT-Systeme, sondern deren Benutzer, um diesen sensible Informationen zu entlocken oder sie zu sicherheitskritischen Handlungen zu verleiten. Dies stellt oftmals die erste Phase einer größeren Cyber-Attacke dar.

Zu den wichtigsten und gleichzeitig ungünstigsten Persönlichkeitsmerkmalen, die ausgenutzt werden, zählen Hilfsbereitschaft, Unerfahrenheit, Gutgläubigkeit, Neugier, Gier oder der Wunsch nach Liebe. Je genauer die potenziellen Opfer im Vorfeld ausgespioniert werden, desto größer sind anschließend die Erfolgsaussichten.

Eine Studie hat gezeigt, dass alleine durch eine personalisierte Anrede in einer gefälschten Mail die Erfolgsquote zum Öffnen eines gefährlichen Links oder eines verseuchten Dateianhangs von 20 Prozent auf 56 Prozent steigen kann. Hilfreich für Human Hacker sind in diesem Zusammenhang vor allem die sozialen Medien wie Facebook, Instagram und X. Wer in diesen Medien viel Privates preisgibt, braucht sich über entsprechend vertraulich anmutende Mails nicht zu wundern.

Während die meisten Angriffe über gefälschte Mails und Webseiten laufen und dabei vor allem die Unerfahrenheit der Benutzer ausnutzen, zielen bspw. auf dem Mitarbeiterparkplatz scheinbar zufällig liegende gelassene und manipulierte USB-Sticks auf die menschliche Neugier ab.

Prominente Beispiele für erfolgreiche Social Engineering-Angriffe sind täglich der Presse zu entnehmen. Zu den spektakulärsten Fällen gehört bspw. der Angriff auf Hillary Clinton in deren Wahlkampf um die amerikanische Präsidentschaft. Damals fiel ihr Wahlkampfmanager auf eine gefälschte Mail herein und gab die Zugangsdaten zu ihrem Postfach preis. In der Folge wurden zahlreiche Mails von Hillary Clinton veröffentlicht.

Security Awareness-Schulungen als essenzieller Baustein für mehr IT-Sicherheit

Wenn technische Maßnahmen alleine also höchstens ausreichen, um IT-Systeme zu schützen, nicht aber deren menschliche Benutzer, bedarf es zusätzlicher Maßnahmen. Dies sind sogenannte Security Awareness-Schulungen, um das Sicherheitsbewusstsein aller Mitarbeiter regelmäßig zu schulen und das richtige Abwehrverhalten im Angriffsfall anzutrainieren. Solche Schulungen können klassische „Klassenraumschulungen“ sein oder auch online erfolgen. Wichtig in beiden Fällen ist aber eine Teilnehmerquote nahe 100 Prozent.

Die Inhalte der Security Awareness-Schulungen können vielfältig sein, müssen regelmäßig wiederholt und immer wieder an neue Angriffsmuster angepasst werden.

Mitarbeiter sollten lernen...

- Internet-Adressen (URL) richtig zu verstehen und im Zweifelsfall zu misstrauen,
- mit Mails generell skeptisch umzugehen, den vermeintlichen Absendern gegebenenfalls zu misstrauen, auf die Anrede zu achten, Nötigungen oder Drohungen zu ignorieren und vor


Social Engineering


Der Mensch ist das schwächste Glied in der Sicherheitskette.





Social Engineering ist die psychologische Manipulation von Menschen, um Handlungen auszuführen oder vertrauliche Informationen preiszugeben.

Schützen Sie sich gegen Social Engineering und errichten Sie eine menschliche Firewall:

 - Gehen Sie verantwortungsvoll mit sozialen Netzwerken um.

- Geben Sie keine vertraulichen Informationen über den Arbeitgeber und die Arbeit in privaten und beruflichen sozialen Netzwerken preis. 

 - Teilen Sie Passwörter, Zugangsdaten oder Kontoinformationen niemals per Telefon oder E-Mail mit.

 - Vorsicht bei E-Mails generell, auch von anscheinend bekannten Absendern. Jeder Angreifer kann sich als jeder Absender ausgeben. Keine Office-Anhänge öffnen und im Zweifel telefonisch rückfragen.

allem Links in Mails am besten zu ignorieren, da das tatsächliche Ziel dieser Links ganz einfach zu verschleiern ist,

- sichere Kennwörter zu benutzen (siehe Infobox),
- den Bildschirm beim Verlassen des Büros zu sperren und auch
- im privaten Umfeld die gleichen Vorsichtsmaßnahmen walten zu lassen.

Social Engineering-Audit als Weckruf für das eigene Unternehmen

In vielen Fällen konzentrieren sich aber die Bemühungen der Unternehmen um mehr IT-Sicherheit leider immer noch ausschließlich auf technische Maßnahmen. Weniger aus Unwissenheit, vielmehr aus einem trügerischen Gefühl der Sicherheit vernachlässigen viele Organisationen dieses wichtige Thema Security Awareness. Es bedarf also offensichtlich einer besonderen Motivation bzw. eines entsprechenden Weckrufs. Dieser Weckruf kann im Rahmen eines sogenannten Social Engineering-Audits erfolgen. Dieses Audit zeigt auf, wie es tatsächlich um das IT-Sicherheitsbewusstsein im Unternehmen steht. Das Audit erbringt dabei in der Regel den Beweis, dass eben doch nicht alle Mitarbeiter mit den Gefahren vertraut sind, die von Social Engineering ausgehen.

Die Aufgabe lautet also, mit klassischen Social Engineering-Methoden die Erfolgswahrscheinlichkeit eines echten (böartigen) Angriffs einzuschätzen. Dieser simulierte Angriff durch die (guten) Auditoren kann dabei per Mail, vor Ort am Unternehmenssitz und/oder per Telefon erfolgen. Ziel des Angriffs sollten möglichst viele Mitarbeiter sein, um eine gute Einschätzung des durchschnittlichen Gefahrenpotenzials zu erlangen.

Um das Ergebnis nicht zu verfälschen, ist es wichtig, keine Insiderinformationen zu verwenden. Die Auswertung des simulierten Angriffs erfolgt anonym ohne jeglichen Hinweis auf die Mitarbeiter und deren positives oder negatives Verhalten. Im Anschluss werden alle erhobenen Daten wieder vollständig gelöscht.

Sie möchten noch mehr für die IT-Sicherheit in Ihrem Unternehmen tun? Die INFOERVE GmbH berät Sie gerne zu technischen und organisatorischen Maßnahmen. Wir stellen Ihr Unternehmen mit einem umfassenden IT-Sicherheitskonzept von der Analyse der IST-Situation über die Bereitstellung der entsprechenden Sicherheitsinfrastruktur bis hin zur Awareness-Schulung auf sichere Füße. ■



Weitere Informationen finden Sie hier:
www.infoserve.de/it-sicherheit

Passwörter

Was hat Ihr Passwort mit einem Chamäleon zu tun?

Denken Sie sich einen Satz aus, der mindestens eine Zahl enthält, zum Beispiel:



"Meine Lieblingstiere sind Chamäleons mit zwei Hörnern und ihrer einzigartigen Zunge!"

Merken Sie sich nun den ersten Buchstaben eines jeden Wortes und Sie erhalten ein starkes und sicheres Passwort.

MLsCm2H+ieZ!

Ein gutes Passwort...

- ... sollte mindestens acht Zeichen lang sein, je länger desto besser.
- ... besteht nicht aus einer Kombination mit Geburtstagen oder Namen des Haustieres.
- ... sollte nicht im Wörterbuch stehen.
- ... darf keine gängigen Wiederholungs- oder Tastaturmuster (asdfgh oder 1234abcd) enthalten.
- ... ist kein simples Passwort, das einfach um ein Sonderzeichen am Anfang oder Ende ergänzt wird.
- ... kann aus Groß- und Kleinbuchstaben, Sonderzeichen (?!%+) und Ziffern bestehen.



INFOERVE
>eurodata-Gruppe

INFOERVE GmbH
Am Felsbrunnen 15
D-66119 Saarbrücken
Telefon +49 681 88008-0
Telefax +49 681 88008-33
www.infoserve.de
info@infoserve.de