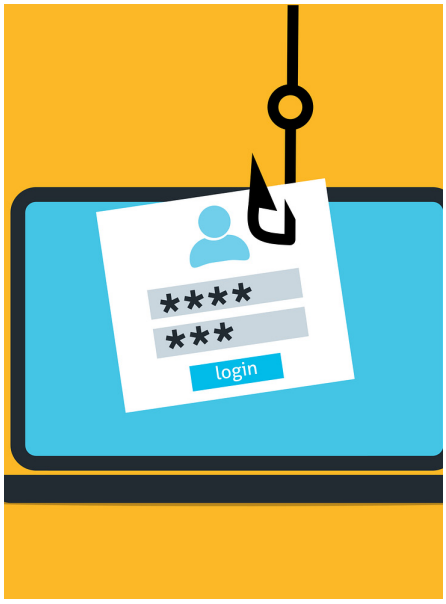
GU Sicherheit & Krisenmanagement

Besser Vor- als Nachsicht. Mit Sicherheit.

Die aktuelle Krise mit der Kriegssituation in der Ukraine zeigt uns auch das Schadenspotential von gezielten Cyberangriffen auf Staaten, Unternehmen oder Privatpersonen. Die Angriffe häufen sich und das Schadens- bzw. Eskalationspotential ist enorm. Schützen Sie sich, es ist wichtig. Mit Sicherheit.

von Priska Schwander



Aktuell hören und lesen wir fast täglich von Cyber- oder Hackerangriffen gegenüber Unternehmen, Gemeinden oder kritischen Infrastrukturen. Was viele jedoch verdrängen – es kann auch uns selbst treffen! Die Digitalisierung hat in unserem privaten, wie auch beruflichen Alltag Einzug gehalten. Computer, Tablets, Handys oder W-LAN sind fast nicht mehr wegzudenken. Einer der häufigsten Irrtümer ist, jemand sei als Privatperson oder Unternehmen zu klein und uninteressant für solche Angriffe, denn es kann uns auch indirekt treffen.

Wer kennt es nicht, kurz vor Feierabend kommt noch eine E-Mail mit einem Anhang von Ihrem Vorgesetzten mit der dringenden Bitte, dies noch kurz zu bearbeiten. Oder wir erhalten eine SMS mit einer Anfrage, ob wir an der Zufriedenheitsumfrage des Unternehmens, in welchem wir vor wenigen Minuten waren, teilnehmen möchten.

Beim Login des E-Bankings kommt eine Fehlermeldung, da wir uns vermutlich bei der ersten Eingabe vertippt haben und nun ein zweites Mal unsere Login-Daten in die Maske eingeben. Am Flughafen wollen Sie noch kurz ein Ferienfoto versenden und wählen sich ins W-LAN ein...

Kommt Ihnen etwas davon bekannt vor? Diese Beispiele sind nur ein paar wenige Situationen, welche Hackern Tür und Tor zu unseren sensiblen Daten öffnen können. Dies kann zum Verlust von sensiblen oder vertraulichen Daten führen mit gravierenden Folgen, wenn diese in die falschen Hände geraten. Dies alles kann Sie als Privatperson oder auch als Firma treffen. Häufig finden solche Angriffe auf verschiedenen Ebenen statt. Einerseits werden Privatpersonen angegriffen, um beispielsweise Zugangsdaten, Passwörter oder ähnliches zu erhalten. Andererseits ist es auch möglich, dass ein Angriff direkt über Ihren Firmencomputer läuft. Sie können erpresst werden, um so an Firmeninformationen zu gelangen. Wenn die Hacker einmal im System sind, können sie mit verschiedensten Hilfsmitteln weitere Informationen abgreifen – sogar so, dass Sie dies möglicherweise gar nicht bemerken. Wappnen Sie sich für den Ernstfall. Wir sind für Sie da. Mit Sicherheit.

Einige Tipps zum optimalen Schutz Ihrer Daten:

- ☐ Computer mit aktuellen Virenschutzprogrammen und Firewalls schützen
- ☐ Cookies regelmässig löschen
- ☐ Verschiedene Passwörter verwenden und regelmässig ändern
- ☐ Persönliche Angaben aufs Nötigste reduzieren
- ☐ Auf Verschlüsselung der persönlichen Daten achten
- ☐ Nutzung von Ortungsdiensten gut überdenken
- ☐ E-Mails, in welchen Daten verlangt werden sehr kritisch betrachten - ev. beim Sender nachfragen
- ☐ Privatsphäre-Einstellungen anpassen
- ☐ Fotos im Internet nicht öffentlich verbreiten
- ☐ Unterschiedliche E-Mailadressen nutzen
- ☐ Auf verschiedene Suchmaschinen zurückgreifen
- ☐ Berechtigungen von Apps so weit wie möglich beschränken

Über die Autorin

Priska Schwander ist seit November 2021 bei der GU Sicherheit & Partner AG. Sie ist eidg. dipl. Berufsoffizier mit «Diploma of Advanced Studies in Militärwissenschaften» der ETH Zürich. Ausserdem war sie Projektleiterin in der Medizin-Informatik.

Priska Schwander
Consultant

GU Sicherheit & Krisenmanagement

Faktenblatt Phishing E-Mail

Was ist Phishing?

Phishing ist eine Methode, bei der Betrüger hauptsächlich via E-Mail versuchen, an sensible Daten zu gelangen. Sie geben sich dabei mit gefälschten Absenderadressen als Person/Firma oder offizielle Behörde aus. Bei den sensiblen Daten handelt es sich bspw. um persönliche/berufliche Logins/Passwörter, Kreditkarteninformationen, Bankdaten usw.

Wie erkennt man Phishing:

Absender

Um was für eine E-Mail Account handelt es sich?
Habe ich dort ein Benutzerkonto?
Funktioniert mein Account derzeit noch?
Erwarte ich eine E-Mail von diesem Absender?
Ist die Absenderadresse richtig?
Bsp: @post.ch oder @schweizerischepost.ch

Datum / Zeit

Wieso schreibt jemand um 03:00 morgens ein E-Mail?

Anhang

Erwarte ich in diesem E-Mail einen Anhang?
Keine Excel, keine ZIP, PP etc. Files öffnen, die man nicht erwartet oder kennt.

Betreff

Ist der Betreff relevant?
Gibt es Rechtschreibfehler?

Anschreiben

Ist das Anschreiben persönlich oder eine Massenmail?

Text

Gibt es Rechtschreibfehler?
Ist der Text persönlich geschrieben oder allgemein?
Gibt es Drohungen oder Forderungen?

Hyperlink

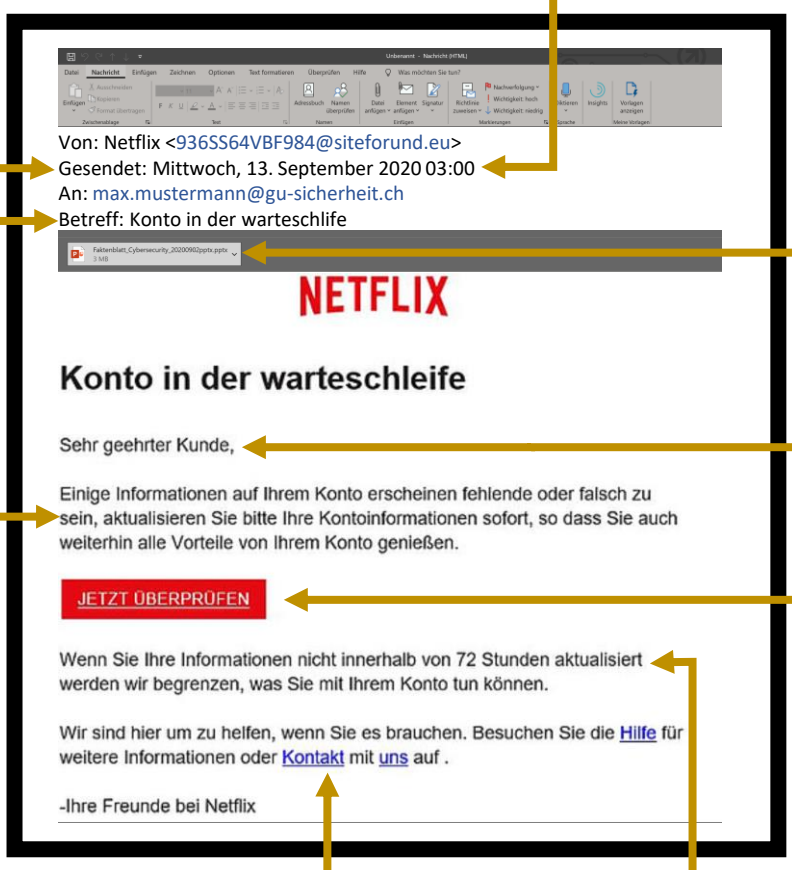
Sind Hyperlinks plausibel in diesem E-Mail?
Wohin führt der Hyperlink? (Mouse-over)

Downloads

Wieso muss ich etwas Downloaden?

Zeitfenster

Wieso gibt es ein so kurzes Zeitfenster?
Werde ich unter Druck gesetzt?



Im Zweifelsfall:

- Nichts anklicken → mit dem IT Verantwortlichen schauen
- Bei der Absenderfirma anfragen, ob sie etwas versendet haben

Nützliche Links:

https://www.ncsc.admin.ch/ncsc/de/home.htm