VOA • Max-Joseph-Straße 5 • D-80333 München

Verband für die Oberflächenveredelung von Aluminium e.V.

ZAC-Tipps gegen Phishing

Mitarbeiterinnen und Mitarbeiter der **Zentralen Anlaufstelle Cybercrime (ZAC)** des Bayerischen Landeskriminalamts bieten regelmäßig Trainings rund um das Thema IT-Kriminalität an. Hier sind ein paar wichtige Tipps der ZAC, wie sich Phishing-Mails enttarnen lassen:

1. Genau hinsehen
   Sehr häufig nutzen Angreifende Buchstabendreher, um seriöse Absender vorzutäuschen. Aus „amazon“ wird dann „amaz0n“ oder „arnazon“. Gerade in kleiner Schrift auf dem Smartphone, bei schlechten Lichtverhältnissen oder in Eile und Hektik fallen Anwender*innen auf diesen Trick herein.

2. Links überprüfen
   Fordert der Absendende dazu auf, auf einen bestimmten Link zu klicken, lohnt es sich diesen erst mal genauer unter die Lupe zu nehmen. Dafür müssen Anwender*innen mit dem Mauszeiger über das entsprechende Wort fahren – OHNE zu klicken. Häufig lässt sich schon darüber erkennen, ob der Link tatsächlich zu der angekündigten Stelle führt oder auf eine andere Domain.

3. Aufbau einer URL kennen
   Der Uniform Ressource Locator, kurz URL, ist der Adressstandard für Websites im Internet. Wer den korrekten Aufbau einer URL kennt, kann Betrüger schnell enttarnen. Es ist das Wort vor dem dritten Schrägstrich (Slash), das den Eigentümer der URL anzeigt.

   Beispiele:
   https://www.amazon.de
   https://primenow.amazon.de/
   https://amazon.schnell-versenden.de/
   https://developer.paypal.com/docs/payout

4. Vorsicht Anhang
   Malware gelangt oft über einen E-Mail-Anhang ins Netzwerk. Hilfreich ist es, die Risikostufen unterschiedlicher Dateitypen zu kennen: Besondere Vorsicht ist bei .exe-Dateien geboten, da es sich um eine ausführbare Datei handelt, über die Schadcode sofort gestartet werden kann. Auch doc.-Dateien sind besonders riskant, wenn die Makros aktiviert wurden. Bei pdfs gelingt das Einschleusen von Schadsoftware meist nur über Sicherheitslücken im System. txt-Dateien sind plain text-Dateien, in denen sich Schadcode nicht ganz so einfach verbergen lässt.

5. Persönliche Rücksprache
   Verlangt ein Geschäftspartner beispielsweise die Änderung der Kontoverbindung, oder die rasche Überweisung hoher Beträge, kann sich der Griff zum Telefon durchaus lohnen, um den Sachverhalt abzuklären. Beim erfolgreichen Payment

Fraud lotsen Betrüger enorme Summen auf eigene Konten, die nach Geldeingang umgehend gelöscht werden.

6. Sprache überprüfen
   Die Zeiten, in denen betrügerische E-Mails in holprigem Deutsch daherkamen, sind leider vorbei. Trotzdem lohnt es sich, die Sprache genau anzusehen: Baut der Absendende unüblich hohen Druck auf, beispielsweise durch sehr kurze Fristen oder Löschungsandrohung eines lange bestehenden Kontos? Auch in solchen Fällen ist es hilfreich, auf der Website des jeweiligen Anbieters die Forderung zu überprüfen oder anzurufen.

7. Technische Schutzmaßnahmen
   Firewall, Anti-Virenschutz und regelmäßige Systemupdates sind neben allen Vorsichtsmaßnahmen eine weitere sinnvolle Möglichkeit, den Rechner und die Netzwerke vor Übergriffen zu schützen.

Geschäftsführerin:
Dr. Alexa A. Becker
Telefon: +49 89 5517 8670
info@voa.de, www.voa.de

HypoVereinsbank
SWIFT/BIC: HYVEDEMM460
IBAN: DE86 7602 0070 1560 3513 79
VAT/USt-ID-Nr.: DE265340572