baramundi

Computersicherheit beginnt am Arbeitsplatz!

Cyberkriminelle sind in den seltensten Fällen Genies oder Computerzauberer. Stattdessen sind es Trickbetrüger, die jahrhundertealte Taktiken verwenden, um sich das Vertrauen ihrer Opfer zu erschleichen. So bringen sie einzelne Anwender dazu, ihnen Zugang zu ihrem IT-Netzwerk zu geben, um dort Daten zu stehlen oder unbrauchbar zu machen.

Fünf einfache Tipps für End User

DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2022

Top 3-Bedrohungen je Zielgruppe

Gesellschaft

Identitätsdiebstahl
Sextortion
Fake-Shops im Internet

Wirtschaft

Ransomware
Schwachstellen
IT-Supply-Chain: Abhängig

Staat und Verwaltung

Ransomware, APT
Schwachstellen, offene oder falsch konfigurierte Online-Server

Die Anzahl der Schadprogramme steigt stetig.
Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

116,6 Mio.

zugenommen.

20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem Zuwachs von 10% gegenüber dem Vorjahr.

34.000

Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000

neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69%

aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z. B. Phishing-Mails und Mail-Erpressung.

90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d. h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

Quelle: Die Lage der IT-Sicherheit in Deutschland 2022, BSI

AUF FOLGENDE TRICKS SOLLTEN SIE GEFASST SEIN

Phishing

Phishing Angriffe erfolgen zumeist über Textnachricht, Voice- oder E-Mail und geben vor, eine vertrauenswürdige Person/Institution zu sein. Damit horchen sie ihre Opfer nach wichtigen Informationen aus (z.B. Login Daten, Kontonummern, oder persönliche Informationen der Anwendenden). Beim CEO Fraud beauftragen sie das Opfer direkt, Überweisungen zu tätigen oder Gutscheincodes an sie zu schicken.

Was Sie dagegen tun können

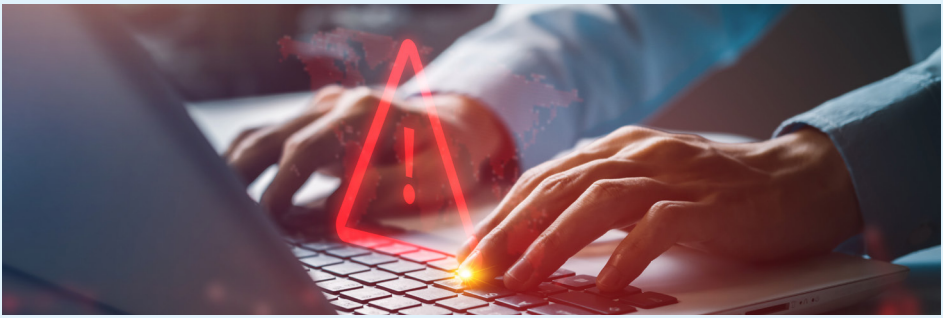
- ✓ Sehen Sie sich Absenderadressen genau an.
- ✓ Ist der Teil hinter dem @ tatsächlich korrekt?
- ✓ Stimmen Absender mit den im Text vorhandenen Links überein?
- ✓ Statt auf Links zu klicken, halten Sie lieber den Mauszeiger ein paar Sekunden darüber, bis die tatsächliche Adresse angezeigt wird.
- ✓ Fragen Sie im Zweifel noch einmal über einen anderen Kanal beim Absender nach.

Ködern (Baiting)

Würden Sie einen auf dem Parkplatz gefundenen USB-Stick an ihren PC anstecken, um zu sehen was darauf ist? Wenn ja, dann sind sie schon in die Falle getappt. Beim Ködern wird die menschliche Neugier ausgenutzt. Denn präparierte Sticks (oder andere Datenträger) enthalten ein Schadprogramm, das so vorbei an allen Firewalls ins Innere des Unternehmens geschmuggelt wird. Auch E-Mail-Anhänge sind ein beliebter Weg, um Malware einzuschleusen.

Was Sie dagegen tun können

- Greifen Sie niemals auf einen Datenträger zu, dessen Herkunft Sie nicht sicher kennen.
- Geben Sie solche Sticks stattdessen direkt bei Ihrem IT-Admin oder CISO ab
- Erklären Sie auch, wie und wo sie ihn gefunden haben.
- Lassen Sie die gleiche Sorgfalt bei Dateianhängen walten.
- Insbesondere passwortgeschützte gepackte/gezippte Anhänge sind verdächtig



Quid pro quo

Hier lässt man das Opfer glauben, es würde illegal einen Vorteil erlangen. So verschickt z.B. ein vermeintlicher Kollege einen Link zu begehrter Software. Die Anti-Virus-App warnt vor der unsicheren Seite, aber das scheinbare Schnäppchen lässt das Opfer die Warnung ignorieren. Selbst wenn dann klar ist, dass etwas nicht stimmt, verhindern Scham und Angst, dass das Opfer zuständige Stellen warnt. Das gibt den Kriminellen mehr Zeit zu agieren.

Was Sie dagegen tun können

- Vertrauen Sie Ihren IT-Admins.
- Angebote, die zu gut klingen, um wahr zu sein, sind es meistens auch.
- Wer illegale Inhalte in der Arbeit nutzt, macht sich grundsätzlich angreifbar.
- Wer hingegen die IT-Admins rechtzeitig warnt, wenn versehentlich der falsche Link geklickt wurde, dem passiert auch nichts.
- Einen Fehler zu verheimlichen, macht ihn nur schlimmer.

Achtung – Dringend

„Dringend! Überweisen Sie bitte sofort 10.000€ an den Lieferanten XYZ, oder wir werden verklagt!“ Bei einer solchen Nachricht will niemand am Ende schuld sein, wenn dann die prophezeite Katastrophe eintritt. Viele Betrugsmaschen funktionieren nur deshalb, weil sie ihre Opfer emotional so unter Zeitdruck setzen, dass sie keine Gelegenheit haben zu hinterfragen und nachzudenken. Erst dadurch wird das sprichwörtliche „unüberlegte Handeln“ ermöglicht.

Was Sie dagegen tun können

- ✓ Einen Gang zurückschalten – der Zeitdruck Ihres Gegenübers ist nicht Ihr Zeitdruck.
- ✓ Nehmen Sie sich mindestens fünf Minuten zum Nachdenken
- ✓ Unerwartete oder ungewöhnliche Anfragen sollten immer hinterfragt werden
- ✓ Holen Sie sich ggf. eine Bestätigung vom vermeintlichen Absender.
- ✓ Nutzen Sie einen separaten Kanal für die Rückfrage (z.B. Telefon bei einer verdächtigen E-Mail)

Höfliches Bitten

Soziales Verhalten wird von Kriminellen gerne ausgenutzt. Es kostet große Überwindung, einer nachfolgenden Person nicht aus Prinzip die Tür aufzuhalten – selbst, wenn sie in einen sensiblen Bereich führt. Der Bitte des angeblichen Admins, sich auf den Computer aufschalten zu dürfen, werden die Meisten ebenfalls nachkommen. Selbst die Frage nach einem Passwort, beantworten viele Anwender wahrheitsgemäß, nur um nicht unhöflich zu erscheinen.

Was Sie dagegen tun können

- ✓ Lassen Sie immer Vorsicht walten, wenn Sie Ihr Gegenüber nicht persönlich kennen
- ✓ Seien Sie bereit, nicht gemocht zu werden, auch wenn es Ihnen schwerfällt.
- ✓ Trainieren Sie sich, soziale Konventionen zu hinterfragen, wenn Sie in sensiblen Bereichen unterwegs sind.
- ✓ Nutzen Sie den Satz „Tut mir leid, die Vorschriften verbieten das.“
- ✓ Melden Sie aufdringliches Verhalten.

Wer diese Verhaltensweisen verinnerlicht und aus Prinzip im Alltag anwendet, ist vor einen Großteil der Social Engineering Angriffe geschützt. Dennoch ist beständige Wachsamkeit gefragt: Kriminelle lassen sich beständig neue Tricks einfallen, um an ihr Ziel zu kommen.

Mehr Informationen zu Cybersicherheit und Schwachstellenmanagement finden Sie auf unserer Webseite

www.baramundi.com/cybersecurity

SICHER DANK STARKER PARTNER

Endpoint Protection von baramundi ist ein elementarer Baustein im Aufbau Ihrer individuellen IT-Security-Strategie. Es sichert den Schutz vertraulicher Daten und damit Vertrauen und Sicherheit Ihrer User an jedem einzelnen Endpoint.

baramundi Vulnerability Scanner
Finden Sie automatisiert bestehende Schwachstellen

baramundi Defense Control
Steuern Sie native MS Tools wie Bitlocker und Defender Antivirus

baramundi Patch Management
Spielen Sie richtlinienkonform und automatisiert Windows Updates ein

baramundi Managed Software
Updaten Sie flächendeckend 3rd Party Anwendungen mit verteilfertigen Softwarepaketen

baramundi Mobile Devices
Verwalten und sichern Sie all Ihre Android und iOS Geräte und setzen Sie Sicherheitsregeln einheitlich durch

baramundi Disaster Recovery
Sichern Sie komplette Partitionen im laufenden Betrieb und setzten Sie Systeme einfach auf einen definierten Zustand zurück

baramundi Personal Backup
Sichern Sie persönliche Einstellungen und Daten der Anwender und stellen Sie sie auf Knopfdruck wieder her

---

DriveLock ist Spezialist für IT- und Datensicherheit und hat es sich zum Ziel gesetzt, Unternehmensdaten, -geräte und -systeme zu schützen. Dabei setzt DriveLock auf Zero-Trust-Lösungen. baramundi erweitert seine UEM-Lösung um zusätzliche Security Module von DriveLock.

baramundi Device Control
Kontrollieren Sie Zugriff und Datenfluss auf Datenträgern

baramundi Application Control
Verhindern Sie die Ausführung schädlicher Anwendungen

---

macmon bietet seit 2003 herstellerunabhängige, BSI-zertifizierte Lösungen, die heterogene Netzwerke dank sofortiger Netzwerktransparenz vor unberechtigten Zugriffen schützen. macmon wird schnell und einfach, mit erheblichem Mehrwert für die Netzwerksicherheit, implementiert. Somit ist macmon ein zentraler IT-Baustein bei den Themenfeldern Digitalisierung, BYOD oder Intend Based Networking. Die Anbindung von baramundi UEM an das Network Access Control (NAC) von macmon bietet exzellente Sicherheit für Unternehmensnetzwerke.

Paessler bietet seit 1997 Monitoring-Lösungen zur Optimierung von IT-, OT- und IoT-Infrastrukturen an. PRTG Network Monitor von Paessler ist die preisgekrönte Lösung für leistungsfähiges, kostengünstiges und benutzerfreundliches Unified Monitoring. Mit Paessler zusammen hat baramundi das gesamte Netzwerk von Endpoint bis Server im Blick – von Monitoring bis zum aktiven Management.