IT-SICHERHEIT · WEITERBILDUNG FÜR IHR UNTERNEHMEN

Der Mensch als Schwachpunkt und Einfallstor.

Eine Firewall lässt sich über Nacht patchen. Ein Mensch nicht – aber schulen.
Genau hier setzt dieses Training an, nicht bei noch mehr Technik.

WIE GEHEN HACKER VOR – UND WAS TREIBT SIE AN?

Die wenigsten Angriffe knacken eine Firewall. Die meisten gehen den einfacheren Weg: über einen Menschen, der eine Tür freiwillig öffnet. Die Motivation dahinter ist selten kompliziert – meistens Geld, manchmal Sabotage oder Konkurrenzausspähung, gelegentlich einfach Neugier.

> *„Guten Tag, IT-Support hier, wir haben ein akutes Problem mit Ihrem Konto – ich brauche kurz Ihren Bestätigungscode, sonst sperren wir Sie aus Sicherheitsgründen." - Kein IT-Support hatte angerufen. Der Zugang war weg, bevor jemand misstrauisch wurde.*

WARUM IST DER MENSCH DER SCHWACHPUNKT?

Nicht, weil Menschen dumm sind – sondern weil genau die Eigenschaften ausgenutzt werden, die im Job erwünscht sind: Hilfsbereitschaft, Respekt vor Autorität, der Wunsch, schnell zu reagieren. Eine Software lässt sich patchen, sobald eine Lücke bekannt ist – dieser menschliche Reflex nicht auf Knopfdruck, aber er lässt sich trainieren.

WIE VERMEIDET MAN PROBLEME?

- ✓ Absender genau prüfen – nicht nur den angezeigten Namen, sondern die echte Adresse/Nummer.
- ✓ Bei Druck, Eile oder Drohung erst recht misstrauisch werden – genau das ist der Trick.
- ✓ Im Zweifel zurückrufen – über eine selbst nachgeschlagene Nummer, nie über die aus der Nachricht.
- ✓ Links nicht direkt anklicken – Adresse selbst eintippen oder eigenes Lesezeichen nutzen.
- ✓ Zwei-Faktor-Authentifizierung überall aktivieren, wo sie angeboten wird.
- ✓ Updates zeitnah einspielen, statt sie wochenlang wegzuklicken.

WER IST SCHULD, WENN ETWAS PASSIERT?

Die naheliegende Antwort – „der Mitarbeiter, der geklickt hat" – bringt nichts und verschlimmert das eigentliche Problem:

- ✗ Den Mitarbeiter bloßstellen, der auf einen guten Trick hereingefallen ist.
- ✗ Vorfälle mit Vorwürfen statt mit Hilfe beantworten.
- ✗ So tun, als könne „das" den eigenen, erfahrenen Leuten nicht passieren.

Angstkultur vertuscht Fehler – der Schaden wächst unbemerkt weiter. **Meldekultur meldet Fehler sofort – der Schaden lässt sich rechtzeitig begrenzen.** Die Verantwortung liegt am Ende bei der Unternehmensführung, nicht bei der einzelnen Person.

EHRLICH GESAGT

Für wen sich das lohnt – und für wen nicht. Ich verkaufe niemandem etwas, das nicht passt:

PASST GUT, WENN …

- ✓ Ihr Team arbeitet mit E-Mail, Telefon oder digitalen Zugängen im Alltag
- ✓ Ihnen echte Sensibilisierung wichtiger ist als eine reine Technik-Checkliste
- ✓ Sie eine Meldekultur statt einer Angstkultur aufbauen möchten

PASST NICHT, WENN …

- ✗ Sie eine rein technische IT-Sicherheitsberatung suchen
- ✗ Sie 08/15-Standardfolien von der Stange erwarten
- ✗ Fehler in Ihrem Haus grundsätzlich bestraft statt gemeldet werden sollen

INDIVIDUELL FÜR IHR UNTERNEHMEN

Jede Schulung wird auf Ihr Unternehmen zugeschnitten – anhand echter, aktueller Beispiele statt auswendig gelernter Regeln oder Angst-Folien. Bei Bedarf starte ich mit einer anonymen Umfrage im Team, um genau dort anzusetzen, wo die größte Wirkung entsteht.

RAHMENDATEN AUF EINEN BLICK

PREIS	3.990 € netto zzgl. Anfahrt
TEILNEHMER	bis zu 12 Personen
DAUER	6–8 Stunden, vor Ort in Ihrem Unternehmen
INHALT	individuell auf Ihr Unternehmen und Ihre Risiken zugeschnitten

WER STEHT DAHINTER

Kein anonymes Schulungsunternehmen: Ich bin Tobias Völzke, Einzelunternehmer, und stehe mit meinem Namen persönlich für jede Schulung gerade. Sie sprechen direkt mit dem Trainer selbst – Chefsupport ohne Warteschleifen und ohne Umwege.

JETZT KOSTENLOSE UND UNVERBINDLICHE BERATUNG SICHERN

Tobias Völzke

Schadesweg 12 · 20537 Hamburg

Telefon: +49 (0)40 333 55 666

E-Mail: tv-mail-2263@tobiasvoelzke.net

https://TobiasVoelzke.net