Ein Moment der Unaufmerksamkeit, fehlende Schutzmaßnahmen oder ein schlecht konfiguriertes Betriebssystem, all das hilft Hackern, in Ihr System einzubrechen. Mit unseren Checklisten sichern Sie Ihre Geräte in wenigen Minuten ab und verhindern Schlimmeres im Falle einer Infiltration.

Von Wilhelm Drehling

Künstliche Intelligenz (KI) überrollt förmlich das Netz und schleicht sich immer mehr in den Alltag hinein. Die neuen KI-Helferlein unterstützen beim Schreiben, beantworten Fragen, retuschieren Bilder, geben aber zum Teil krude, wenn auch glaubhafte Antworten. Deshalb ist es wichtig, kritisch gegenüber den neuen Tools zu bleiben. Auch wenn sie sinnvolle Einsatzmöglichkeiten bieten, empfehlen wir einen vorsichtigen Umgang mit den KI-Werkzeugen. Nicht selten steht in den AGBs, dass die Anbieter sich die von Nutzern gestellten Fragen und hochgeladenes Material einverleiben dürfen, um ihre Tools weiterzuentwickeln. Das ist zwar kein typischer Angriff in Form eines Trojaners oder Hackerangriffs, betrifft aber trotzdem Ihre persönlichen Daten. Mehr dazu lesen Sie auf Seite 75.

Aufgepasst!

Es genügen ein paar Handgriffe, um Ihr Netzwerk, Ihr Smartphone und Ihren Rechner gegen die gröbsten Angriffe zu rüsten. Klar, das ist kein allumfassender Schutz, der Hightech-Viren fernhält. Da aber die meisten Angriffe einfach zu schließende Lücken ausnutzen, sind Sie mit unseren Empfehlungen erstklassig dagegen gewappnet. Außerdem sind die meisten in wenigen Minuten erledigt, so viel Zeit muss sein. Aus diesem Grund haben wir die Security-Checklisten der vergangenen Jahren auf den neuesten Stand gebracht.

Wie Sie es vielleicht schon kennen, sind unsere Empfehlungen thematisch sortiert: Los geht es mit Tipps zum Homeoffice (S. 70). Der Arbeitsplatz zu Hause ist gekommen, um zu bleiben, und sollte aufgrund der direkten Verbindungen ins Netzwerk des Unternehmens besonders geschützt werden. Da geschäftliche Mailkonten nicht selten ein bevorzugtes Ziel von Phishing-Versuchen sind, finden Sie auf Seite 74 Ratschläge, um Betrügermails zu enttarnen. Tipps und Tricks zu Windows (S. 71), Smartphone (S. 72) und WLAN-Router (S. 73) runden das Paket ab.

Auch nach Feierabend haben es Betrüger auf Ihr Geld abgesehen, seien Sie also achtsam bei Transaktionen im Browser (S. 77), vor allem wenn Sie Überweisungen via Onlinebanking (S. 79) erledigen. Nutzen Sie immer eine Zwei-Faktor-Authentifizierung. Passen Sie bei Mails auf, die angeblich von Ihrer Bank stammen und Sie dazu auffordern, Ihre Anmeldedaten zu bestätigen. Es handelt sich hierbei häufig um raffinierte Phishing-Versuche!

Ein falscher Klick und schon sind die Bilder vom letzten Urlaub weg oder schlimmer noch wichtige Dokumente wie Steuerunterlagen. Daten, die Sie schützen möchten, sollten Sie absichern und zusätzlich in Form eines Backups aufbewahren (S. 80) – ein USB-Stick reicht aus. Sollten Sie zudem einen eigenen Server (S. 81) betreiben, müssen Sie sichergehen, dass dieser immer auf dem aktuellen Stand ist. Loggen Sie sich stets via SSH ein und verwenden Sie anstatt eines Passworts lieber das Public-Key-Verfahren.

Auch wenn mit Passkeys [1, 2] Passwörter obsolet werden dürften, sollten Sie nach wie vor schwierige Passwörter wählen oder einen vertrauenswürdigen Passwortmanager benutzen (siehe S. 82). Und noch ein guter Rat: Bewegen Sie sich vorsichtig auf den üblichen Messengerdiensten (S. 76) sowie diversen Social-Media-Plattformen (S. 78) und glauben Sie nicht jeder eintrudelnden Nachricht. Betrüger denken sich immerzu neue perfidere Maschen aus (siehe Screenshot links).

Seien Sie auf der Hut bei SMS-Nachrichten, die zum Kontakt mit anderen Nummern auffordern und kontaktieren Sie zur Sicherheit über Zweitkanäle Familie und Verwandte, um die Herkunft der SMS zu bestätigen.

Weitergeben

Damit sich unsere Tipps möglichst weit herumsprechen, haben wir sie in einem kostenfreien PDF-Booklet zusammengefasst. Dieses können Sie über ct.de/ytrq herunterladen und dann nach Belieben an Freunde, Familie und Bekannte verteilen. Und nun ran ans Werk! *(wid@ct.de)* c't

Literatur

[1] Kathrin Stoll, Tschüss Passwort?, So funktionieren Passkeys, c't 26/2022, S. 126
[2] Ronald Eikenberg, Zukunft ohne Passwort, Bestandsaufnahme: Passwort-Nachfolger Passkeys, c't 13/2023, S. 12

PDF-Booklet kostenfrei herunterladen:
ct.de/ytrq