Windows absichern – Das Praxis-Handbuch

Leseprobe – Kapitel 1 (Auszug)

Hast du dich jemals gefragt, warum dein Windows-PC trotz Updates und Antiviren-Software plötzlich zum Ziel von Phishing-Angriffen oder Erpressungstrojanern werden kann? In diesem praxisnahen Handbuch lernst du Schritt für Schritt, wie du deine Maschine mit den gleichen Sicherheitsmaßnahmen schützt, die große Unternehmen einsetzen – ohne IT-Vorkenntnisse.

Warum Angriffe nicht nur Firmen treffen

Kaum ein Tag vergeht, an dem nicht über Datenlecks, Ransomware-Banden oder gehackte Online-Shops berichtet wird. Die Schlagzeilen klingen oft nach Konzernen, Behörden oder Krankenhäusern – also nach Zielen, die ohnehin über IT-Profis, Budgets und Notfallpläne verfügen. Daraus entsteht bei vielen Privatpersonen ein verhängnisvoller Trugschluss: „Mich betrifft das nicht. Ich habe nichts zu verbergen, und mein Rechner ist für Kriminelle ohnehin uninteressant.“

Beide Annahmen sind falsch. Angreifer denken nicht in Schubladen wie „wichtig“ oder „unwichtig“. Sie denken in Zahlen: Wer Millionen von Privatgeräten gleichzeitig mit einer einzigen Phishing-Welle erreichen kann, muss nicht jedes einzelne Opfer aussuchen. Es reicht, wenn ein Bruchteil hereinfällt.

Auf einem typischen Windows-Heimcomputer lagern heute Dinge, die vor zehn Jahren noch in Papierordnern oder Fotoalben lagen: Steuererklärungen, Kontoauszüge, Scans des Personalausweises, Krankenversicherungs-nummern, Zugangsdaten zu Streaming-Diensten, Familienfotos in der Cloud. Für Kriminelle ist das ein Eldorado – sie können daraus direkt Geld machen:

- **Kontozugriff:** Mit erbeuteten Online-Banking-Daten werden Überweisungen ausgelöst.
- **Erpressung:** Verschlüsselte Dateien oder kompromittierte Konten werden gegen Lösegeld freigegeben.
- **Identitätsübernahme:** Im Namen des Opfers werden Einkäufe getätigt, Konten eröffnet oder Kredite beantragt.
- **Weiterverkauf im Darknet:** Personenbezogene Datensätze erzielen auf Untergrundmärkten Cent- bis Euro-Beträge pro Eintrag.

Allen typischen Vorfällen ist gemeinsam, dass kein besonders tiefes Fachwissen nötig war, um sie auszulösen – ein einziger unbedachter Klick genügt. Genau deshalb ist Windows-Sicherheit zu Hause keine Spezialistendisziplin, sondern eine alltägliche Grundaufgabe, vergleichbar mit dem

Merke. Privatanwender sind kein Randthema der IT-Sicherheit, sondern ein Hauptziel. Automatisierte Angriffe treffen jeden, der online geht. Der Unterschied liegt nicht in der „Wichtigkeit“, sondern in der Vorbereitung.

Phishing – gefälschte Nachrichten mit echtem Schaden

Phishing bezeichnet den Versuch, mit gefälschten Nachrichten an vertrauliche Informationen zu gelangen. Klassisch ist die E-Mail, die nach Log-in-Daten für die Sparkasse, PayPal, die DHL-Sendungsverfolgung oder Microsoft 365 fragt. Die Links sehen auf den ersten Blick seriös aus, führen aber auf nachgebaute Webseiten. Heute funktioniert die Methode nicht mehr nur per E-Mail, sondern ebenso per SMS („Smishing“), per WhatsApp-Nachricht, per QR-Code auf Parkautomaten oder Aushängen und zunehmend über Social-Media-Direktnachrichten.

Was Phishing so gefährlich macht, ist die Mischung aus Zeitdruck und persönlicher Ansprache. Sätze wie „Ihr Konto wird in 24 Stunden gesperrt“ oder „Wir haben eine ungewöhnliche Anmeldung festgestellt“ sollen verhindern, dass man in Ruhe nachdenkt. Wer die Nachricht genau prüft, findet fast immer Hinweise: eine kryptische Absenderadresse, eine ungewohnte Anrede, oder eine Domain wie `sparkasse-sicherheit-pruefung.de` statt `sparkasse.de`.
