IT-TIPP

essendi it
IT-Beratung und -Entwicklung

Gewappnet vor Hackerangriffen?

Die Methoden werden immer raffinierter, keine Sicherheitslücke bleibt ungenutzt

Immer wieder sorgen Hacker mit ihren Angriffen für Schlagzeilen in den Medien. Dabei haben sie es immer häufiger auch auf kleine und mittlere Privatunternehmen abgesehen. Und sie beschränken sich dabei nicht auf Ballungszentren.

Hacker haben es nicht nur auf Regierungsdaten abgesehen. Auch in Privatunternehmen sorgen ihre Angriffe für Arbeitsausfälle, weil IT-Systeme aus Sicherheitsgründen abgeschaltet werden müssen. Schlimmstenfalls werden Daten gestohlen. Der Landesdatenschutzbeauftragte sowie das Landeskriminalamt werden eingeschaltet, um Sicherheitslücken zu finden.

Hackerangriffe begegnen uns täglich. Weit verbreitet ist **Phishing**. Dabei wird der Nutzer etwa per E-Mail aufgefordert, Passwörter oder Kontodaten zur Bestätigung der Identität auf einer täuschend echt nachgeahmten Webseite einzugeben. Mit den so ergaunerten Zugangsdaten ziehen Cyberkriminelle z.B. Gelder ab.

Anfang des Jahres las man häufig, dass Computerdaten durch Schadsoftware verschlüsselt wurden. Erst nach Zahlung einer Lösegeldsumme sollten sie wieder freigegeben werden. Hierbei handelt es sich um Attacken mit **Ransomware** (ransom = Lösegeld). In Unternehmen kann der Schaden immens sein, wenn Daten dadurch unwiederbringlich verschwinden.

Kennungen und Passwörter werden auch in sogenannten **Brute-Force-Angriffen** geknackt. Dazu setzen Hacker Programme ein, die mit roher Gewalt (brute force) Kennwort- bzw. Tastenkombinationen ausprobieren.

Die Liste ließe sich leider erweitern. Und wie schützt man sich vor Datenklau?

Wichtig: Hackern keine Sicherheitslücken bieten. Programme und Komponenten immer auf dem neuesten Stand halten und Sicherheitsupdates zeitnah einspielen.

Namen, Geburtsdaten, etc. sind leicht zu entschlüsselnde Passwörter. Je kryptischer und zufälliger die Kombination, desto sicherer ist sie. Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, am besten bunt durcheinandergewürfelt! Schwierig zu merken? Dafür schwerer zu knacken! Je länger Malware benötigt, um ein Passwort zu entschlüsseln, umso höher ist die Chance, dass der Angriff bemerkt wird.

Keine Mailanhänge öffnen, die man nicht erwartet hat. Schon gar nicht, wenn es sich um ausführbare Dateien handelt. Durch das Öffnen werden darin versteckte Viren ins System geschleust. Statt eine vermeintliche Rechnung aufzumachen, erstmal in der Einkaufsabteilung nachfragen!

Bevor man auf einer Webseite Nutzernamen, Passwörter, Kreditkarten- oder Kontoinformationen eingibt, die URL genau unter die Lupe nehmen. Sieht sie verdächtig aus, ist ein unauffälliger Schreibfehler enthalten? Dann besser keine Daten preisgeben.

Echte Unternehmenswebseiten erkennt man z.B. am Schlosssymbol links oben in der Browserzeile. Klickt man darauf, werden zusätzliche Informationen zum digitalen Zertifikat angezeigt, das den Austausch der Daten absichert. Die Übermittlung erfolgt verschlüsselt, ohne dass unbefugte Dritte mitlesen können. Das ist z.B. bei Login-Bereichen wichtig.

In Unternehmen sind vielfältige digitale Zertifikate im Einsatz. Hier ist ein Zertifikatsmanager wie essendi xc ein bedeutender Sicherheitsbaustein. Er überwacht den gesamten Lebenszyklus aller im Betrieb eingesetzten Zertifikate und warnt vor deren Ablauf. Je nach Einstellung verlängert er sie automatisch. Damit trägt er zu hoher Betriebssicherheit bei.

Wir bei essendi it entwickeln IT-Lösungen für Finanzdienstleister, Handel und Industrie auf aktuellem technologischem Niveau. Dabei sind wir spezialisiert auf IT-Sicherheit und Zertifikatemanagement.

essendi it
IT-Beratung und -Entwicklung

essendi it GmbH
Dolanallee 19
74523 Schwäbisch Hall
Telefon 07 91-94 30 70-12
Internet: www.essendi.de