Wie viel Sicherheit lohnt

Passwörter, Firewalls, Verschlüsselung – welche Vorkehrungen für die Firmen tatsächlich notwendig sind.

Klaus Jung hat Glück gehabt, als die Internetseiten seiner Firma Gartenfrisch GmbH gehackt wurden. Unbefugte hinterlegten auf dem Server eine eigene Seite, um an die Adressen und die Kontodaten der Kunden heranzukommen. »Da wir noch keine einzige Bestellung hatten, waren auch noch keine Informationen gespeichert«, erzählt der Lebensmittelhändler erleichtert.

Leider sind solche Phishing-Attacken wie bei Gartenfrisch keine bedauerlichen Einzelfälle. Allein diese Art von Internetangriffen führe in Deutschland zu einem jährlichen volkswirtschaftlichen Schaden in zweistelliger Millionenhöhe, schätzt der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom). »An einem DSL-Anschluss gehen zurzeit mehrere Angriffe pro Minute ein«, warnt Torsten Holz, Virenforscher der Universität Mannheim, eindringlich vor Würmern, Trojanern und anderen Schädlingen.

»Ein aktuelles Antivirenprogramm ist ein absolutes Muss bei jedem Computer mit Internetzugang«, fordert Sicherheitsexperte Michael Schwartzkopff vom IT-Berater Multinet. Auch automatische Software-Updates senken das Risiko vor unbefugten Zugriffen (siehe »Das Pflichtprogramm«). Doch nicht jede Firma ist gleichermaßen von Attacken bedroht. impulse erklärt, welche Vorkehrungen im Einzelfall zu empfehlen sind.

Generell gilt: »Je abhängiger der Betrieb von seiner IT ist, desto effizienter muss die Abschirmung ausfallen«, rät Frank Giesche vom führenden Solinger Netzwerkspezialisten Nonstop Technologies. Sein Tipp zum Beispiel für Besitzer von Online-Shops: Sie sollten einen Provider beauftragen, der sogenannte Managed Server betreibt. Hierbei stellt das speziell geschulte Personal beim Dienstleister ständig sicher, dass potenzielle Sicherheitslücken so schnell wie möglich geschlossen werden. Diesen Service bietet der Berliner Hersteller Strato beispielsweise bereits ab rund 70 Euro monatlich an.

Schadenersatz droht

Eine kostenlose, aber nicht minder wirksame Schutzmaßnahme ist die regelmäßige Auswechslung aller Passwörter. Internethändler, die Kartenzahlungen akzeptieren, sind sogar dazu verpflichtet. »Andernfalls müssen sie für aufgetretene Schäden beim Kunden geradestehen«, erklärt Sicherheitsexperte Schwartzkopff.

Stärkere Vorkehrungen müssen Firmen treffen, wenn Kollegen sich von beliebigen Standorten aus in das Unternehmensnetzwerk einwählen können. In diesen Fällen reicht ein normaler Passwortschutz nicht aus. Besser ist es, zusätzlich sogenannte Security Tokens einzuführen. Sie erzeugen im Minutentakt neue Geheimnummern – so schnell ist der erfahrenste Hacker nicht. Tokens gibt es beim Marktführer RSA Security ab etwa 1800 Euro für zehn Anwender und drei Jahre Nutzungszeit.

Auch Betriebe, die mehrere Filialen verbinden, sollten in ihre IT-Sicherheit investieren. »Nur eine Firewall schützt die Computer wirksam vor dem Zugriff von außen«, erklärt Berater Giesche. Und ein zusätzliches Computer-Netzwerk, neudeutsch Virtual Private Network (VPN) genannt, sorgt dafür, dass sämtliche Daten zwischen den PCs verschlüsselt über das Web übertragen werden.

Händler Jung hat jedenfalls aus der Phishing-Attacke auf seinen Online-Shop gelernt. »Wir sorgen etwa mit regelmäßigen Software-Updates für mehr Sicherheit auf unseren Seiten«, erklärt der Gartenfrisch-Chef.

Achim Wagenknecht ressort.computer@impulse.de

Illustration: Thomas Di Paolo für impulse

Das Pflichtprogramm für den PC-Schutz

Computer mit Internetanschluss werden mehrmals pro Minute angegriffen. Michael Schwartzkopff, Sicherheitsexperte beim Beratungsunternehmen Multinet, erklärt die fünf wichtigsten Schutzmaßnahmen.

1. Die Bestandsaufnahme
Nur wer genau weiß, wo überall im Unternehmen Informationen gespeichert werden, kann diese Ressourcen schützen. So können die Datenquellen im Rahmen eines Workshops gesammelt werden. Vertreter aller Abteilungen sollten daran teilnehmen.

2. Die Software-Updates
Egal ob Betriebssysteme wie Windows und Linux oder Anwendungsprogramme: Wenn eine automatische Update-Funktion vorhanden ist, sollte sie auch aktiviert werden. So werden neu entdeckte Sicherheitslücken garantiert zum Nulltarif geschlossen.

3. Die Firewall
Empfehlenswert sind Geräte, die zunächst alles abblocken und einzelne Freigaben verlangen. Zum Beispiel das Astaro Security Gateway 120 für rund 800 Euro.

4. Die Antivirenprogramme
Ein Schutzprogramm gegen bösartige Software gehört auf jeden Windows-Rechner. Viele Hersteller bieten inzwischen auch Schutz gegen Root-Kits sowie andere Schädlingsprogramme an. Empfehlenswert: das Avira Antivir Small Business Bundle für fünf Nutzer und mit einem Jahr Laufzeit. Der Preis: 365 Euro.

5. Das Bewusstsein
Die meisten Sicherheitslücken lassen sich auf Fehlbedienungen der Mitarbeiter zurückführen. Machen Sie jedem Kollegen klar, welche Folgen es haben kann, wenn er Passwörter bekannt gibt oder eigenmächtig die Antiviren-Software auf seinem PC deaktiviert. Anschauliche Informationen gibt es kostenlos im Internet: etwa beim Bundesamt für Sicherheit in der Informationstechnik.
➜ www.bsi.de/gshb/leitfaden/