Irgendwann wird jeder infiziert

Experten warnen vor immer raffinierteren Cyber-Attacken auf Unternehmen

VON G. LE CLAIRE

Cyber-Kriminalität verursacht jedes Jahr Schäden in Milliardenhöhe, speziell der Mittelstand ist ein beliebtes Opfer. Wo die größten Gefahren lauern und wie man sich wappnet, diskutieren Experten und Aussteller auf der it-sa in Nürnberg, Europas bedeutendster Messe für IT-Sicherheit.

Erste Hilfe nach einem Cyber-Angriff versprechen viele Aussteller auf der it-sa. Früher oder später macht jedes Unternehmen Bekanntschaft mit IT-Kriminellen, so Experten. Foto: Weigert

NÜRNBERG – Ach waren das noch Zeiten, als E-Mails verzweifelter afrikanischer Prinzen in abenteuerlicher Rechtschreibung im Postfach landeten. 10000 € würden sie überweisen, für einen winzigen Freundschaftsdienst. Details über beigefügten Link: klick. Unfreiwillig komisch wirken heute die plumpen Betrugsversuche aus der Steinzeit des IT-Verbrechens.

Inzwischen ist Experten der Spaß vergangen. „Wir beobachten, dass die Qualität der Cyber-Angriffe erheblich steigt", sagt Michael Hange, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), zum Auftakt der it-sa im Nürnberger Messezentrum. 428 Aussteller präsentieren auf Europas größter Fachmesse für IT-Sicherheit noch bis Samstag ihre Gegenmittel von der Bedrohungsanalyse bis zum Krisenmanagement im Ernstfall.

Auf 51 Mrd. € jährlich schätzt der Branchenverband Bitkom den Schaden für die deutsche Wirtschaft durch Cyber-Kriminelle, insbesondere in der Kfz-Industrie, der Chemie- und Pharmabranche sowie im Finanz- und Versicherungswesen. Entgangene Einnahmen durch Plagiate, verletzte Patente, Erpressung mit sensiblen Daten: Für die Betroffenen ist der Ärger groß, und dazu zählte in den vergangenen zwei Jahren nach einer Bitkom-Studie schon gut jedes zweite Unternehmen.

Besonders gefährdet ist der Mittelstand. Verbrecher weltweit wüssten, dass auf deren Festplatten die Daten für Produkte auf Weltniveau lagerten, bei meist relativ überschaubarer IT-Sicherheit. „Zugleich sind Mittelständler als Lieferanten häufig gut in die Systeme von Großkonzernen eingebunden, können Cyber-Kriminellen also als Einfallstor für Attacken auch auf diese dienen", erklärt Bitkom-Experte Winfried Holz.

Verbrechen leicht gemacht

Wobei die Täter keineswegs immer in Russland, China oder den USA sitzen. Laut Bitkom stecken in 52 Prozent der Fälle aktuelle oder ehemalige Mitarbeiter hinter dem Angriff. Denn, auch das ein Trend: Um beispielsweise eine Firmen-Homepage lahmzulegen, braucht heute niemand mehr ein Informatik-Studium. Im Internet gibt es einen wachsenden Markt für Schadsoftware, praktisch in der Anwendung für jedermann.

Angesichts der steigenden Qualität und Quantität der Angriffe raten IT-Experten zu einer geänderten Gegenstrategie. „Früher kam es vor allem auf Prävention an", sagt Bitkom-Experte Marc Fliehe. Doch damit sei es nicht mehr getan: „Es ist heute nur eine Frage der Zeit, bis ein Unternehmen gehackt wird." Schon beizeiten sollten Firmen daher einen Krisenplan aufstellen, um im Ernstfall schnell reagieren zu können und so die Chance zu wahren, den Schaden wenigstens zu minimieren.

Stefan Strobel, Chef der IT-Sicherheitsfirma Cirosec, beobachtet jeden Tag das Treiben im Netz: „Viele Verbrecher geben sich inzwischen richtig Mühe." Mails, die ihre Empfänger zum Klick eines Links verführen sollen, über den sich dann Schadsoftware installiert, kämen beispielsweise im Gewand perfekt gefälschter Amazon-Bestellbestätigungen daher.

Noch perfider seien sogenannte Wasserloch-Angriffe: In der Savanne lauern hier die Krokodile und Löwen, trotzdem müssen Zebras und Gnus dorthin. In der IT-Welt seien Wasserlöcher per Schadcode infizierte Internetseiten, die bei Mitarbeitern einer Firma erfahrungsgemäß beliebt seien. „In den USA ist das zum Beispiel mal der Forbes-Seite passiert. Es hat Monate gebraucht, das überhaupt zu merken."

Da wünscht man sich fast den afrikanischen Prinzen zurück…