Immer mehr Attacken aus dem Internet

Cyberkriminalität: Unternehmen und Verwaltungen müssen viel Zeit aufwenden, um Angriffe auf ihre Computernetzwerke abzuwehren. Andreas Schürkamp vom Herforder Unternehmen DTS-Systeme erklärt, wie man ihnen entgegen wirkt

Von Christian Geisler und Dirk Windmöller

Bedrohung: *Tausendfach am Tag versuchen Hacker, auf Rechner von Unternehmen und Privatpersonen zuzugreifen. Dazu verwenden sie Viren, Trojaner und Würmer. Auch Erpresser sind vermehrt im Netz tätig.* FOTO: GETTY IMAGES

■ **Herford**. Jeden Tag werden Unternehmen und öffentliche Verwaltungen angegriffen. Die Täter sind aber nicht etwa mit Messern oder Pistolen bewaffnet, sondern gehen deutlich subtiler vor – über das Internet. Mit Hilfe von Viren, Würmern und Trojanern lösen sie Chaos aus. Ein Cyberangriff genügt, um die Systeme von Unternehmen lahmzulegen. Die einzige Möglichkeit, Schäden gering zu halten, ist ein wirksamer Schutz.

ALLTÄGLICHE ABWEHR

„Unser Netzwerk wird stündlich durch mehrere 100 Angriffe attackiert", sagt Réne Scherer, Marketingleiter der Firma Steute Schaltgeräte. Die Abwehr von Angriffen aus dem Netz gehöre für das Unternehmen längst zum Arbeitsalltag dazu. „Bei uns ist ein Mitarbeiter aus der EDV mehrere Stunden täglich mit dem Thema Cyberangriffe beschäftigt", sagt Scherer.

Nach Angaben von Andreas Schürkamp, Technischer Leiter des Herforder Unternehmens DTS-Systeme GmbH, das sich deutschlandweit als Spezialist für IT-Sicherheit etabliert hat, hat die Zahl der Angriffe aus dem Netz nicht nur zugenommen, auch die Qualität der Attacken steige. Häufig setzten Täter Spam-Mails oder die so genannte DDoS-Attacke (Distributed Denial of Service) ein.

SPAM-MAILS

Als Spam-Mail werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden. Häufig enthalten sie Links oder Anhänge, die dem Computersystem schaden. „Früher erkannte man anhand der schlechten Rechtschreibung bereits auf einen Blick, ob eine Spam-Mail vorliegt", sagt Schürkamp. „Heute sind die Täter deutlich professioneller geworden."

So lande beispielsweise eine als Nachricht von der Geschäftsführung getarnte Mail bei der Buchhaltung oder der Marketing-Abteilung – deren Mitarbeiter öffnen den Anhang oder Link und infizieren auf diese Weise das Computersystem der Firma. „Das können Viren, Trojaner oder Würmer sein. In jedem Fall etwas, das das System lahmlegt", so Schürkamp. Im Zweifel sollten Mitarbeiter die Absenderadresse genau überprüfen und nur nach Rückfrage Anhänge öffnen.

„Um sich vor Spam und den Schadcodes in der Mail zu schützen, sind gute Prüfmechanismen nötig", sagt der Experte für IT-Sicherheit. Es gebe Software oder Services, mit deren Hilfe Spam-Mails gar nicht erst zugestellt werden oder unerwünschte Links und Anhänge herausgefiltert werden.

Auch Reinhold Harnisch, Geschäftsführer des Kommunalen Rechenzentrums (KRZ) in Lemgo, hält IT-Schutz für unabdingbar. Die Mails, die zum Beispiel an die Stadt Herford und auch an alle anderen Kommunen aus den Kreisen Herford, Minden-Lübbecke und Lippe geschickt werden, landen auf dem Server des KRZ. „Wir filtern 96 Prozent Spam aus den kommunalen Mails heraus", sagt Harnisch.

Experte: *Andreas Schürkamp von DTS-Systeme.* FOTO: DTS SYSTEME

Spam zu öffnen, bedeute immer eine potenzielle Gefahr. Schadsoftware könne zum Beispiel Rechnerleistung klauen. „Außerdem kann der Rechner mit vielen tausend anderen zusammengeschaltet und für einen großen Angriff genutzt werden", so Harnisch. Fachleute sprechen in diesem Zusammenhang von einem BOT-Netz. Die Attacken werden als DDoS-Attacken bezeichnet.

DDOS-ATTACKE

Denial of Service (englisch für „Verweigerung des Dienstes") bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Gründe dafür können einerseits eine Überlastung des Datennetzes oder aber ein gezielter Angriff von Cyberkriminellen sein, die eine Überlastung mutwillig herbeiführen.

Laut Andreas Schürkamp werden sogar Serverbetreiber zu einer Geldzahlung erpresst, damit ihr Internetangebot wieder erreichbar wird. „Die Täter arbeiten mit der Angst. Manchmal reicht die Androhung, ein Angebot lahmzulegen, schon aus, um Unternehmen zur Zahlung zu zwingen", sagt Schürkamp. In der Regel pochen die Täter auf die Überweisung von Bitcoins, einer Online-Währung, die nicht zurückverfolgt werden kann.

Mittlerweile würden solche DDoS-Attacken unter anderem im Darknet zum Kauf angeboten werden, die Käufer können damit zum Beispiel Konkurrenzfirmen schaden. „Es muss nicht einmal ein finanzieller Schaden entstehen. Manchmal führt eine Seite, die vom Netz gegangen ist, auch zu einem Imageverlust für das Unternehmen", erklärt Schürkamp. Aber auch gegen solche Attacken sei ein Schutz möglich. „Es gibt für alle Szenarien Abwehrmechanismen", sagt der Experte. „Allerdings müssen sie vorbeugend implantiert werden. Im Nachgang eines Angriffs ist meist nichts mehr zu retten."