Die IT-Sicherheit im Fokus

MEHR VORSICHT WALTEN LASSEN

Obwohl es Schlagzeilen von Hackerangriffen und Datenklau schon seit Längerem in beängstigender Regelmäßigkeit auf die Titelseiten der Leitmedien schaffen, verhält sich der Großteil der Computer- und Internetnutzer weiterhin vergleichsweise sorglos. Die gefühlte Bedrohungslage hinkt meilenweit hinter der tatsächlichen her, so lautet die Einschätzung von IT-Sicherheitsexperten. Dabei ist jeder Internetnutzer, beruflich wie privat, ein potentielles Opfer. Nur weil man nichts bemerkt, bedeutet das nicht, dass man nicht schon längst selbst betroffen ist.

Türen und Fenster sind weit geöffnet. Auf dem Tisch liegen ausgebreitet Kontoauszüge- und Zugänge, Passwörter, unterschiedlichste Brief- und E-Mail-Konversationen, streng vertrauliche Dokumente, Fotos und Videos, alles findet sich hier. In einem abgelegenen Zimmer des Hauses sitzt der Hausherr mit Augenbinde und Ohrstöpsel versehen und wiegt sich in Sicherheit. Er bemerkt nicht, wie Fremde ungehindert ihr Unwesen treiben, seine Dokumente, Passwörter und sonstige vertrauliche Dokumente lesen, kopieren oder entwenden. Er entdeckt nicht, dass sich ungebetene Gäste dauerhaft in seinem Haus einnisten und von dort aus nun weitere Häuser ausspähen.
Sie denken, das ist ein völlig überzogenes Bild? Zugegeben in der materiellen Welt der Häuser und Straßen, ist dieses Szenario unwahrscheinlich. Absolute Realität ist es aber in der digitalen Welt des Internets, in der Welt der Datenströme und Computer. Dort geschieht ebendies sekündlich und millionenfach. Das Haus ist lediglich als Bild für internetfähige Geräte zu verstehen, in erster Linie Computer und der Hausherr steht für Internetnutzer, privat wie beruflich.

Foto: BRZ

„IT-Sicherheit muss besonders für Unternehmen, aber auch für private Nutzer zum absoluten Standard werden. Das erfordert nicht zuletzt die fortschreitende Digitalisierung", resümiert IT-Sicherheitsexpertin Stefanie Götz.

Info
Was versteht man unter einem Hacker-Angriff?
Ein Angriff ist der Versuch, die Vertraulichkeit, Integrität und Verfügbarkeit bestimmter Daten zu beeinträchtigen. Unter Angriff versteht man:
- Betrug, Diebstahl, Erpressung
- Datenkompromittierung (Zerstörung oder Veränderung von Daten)
- Imagebeschädigung (Reputation)
- Spionage
- Systemmissbrauch (illegitime Nutzung von Ressourcen wie z.B. Internet, Webseiten werden zum Spamversand missbraucht)

Unternehmens-IT braucht besonderen Schutz

Stefanie Götz arbeitet im Rechenzentrum von BRZ Deutschland. Gemeinsam mit zwei Kollegen überwacht die IT-Expertin, ob alle Sicherheitssysteme reibungslos laufen oder ob es Vorkommnisse gibt, die besondere Aufmerksamkeit erfordern. Das BRZ-Rechenzentrum im Herzen Nürnbergs ist sozusagen die materielle Heimat der Cloud für die Bauwirtschaft. Die IT-Experten hier wissen, welche Bedrohungen auf Unternehmen in der virtuellen Welt lauern. Baufirmen und Handwerksbetriebe speichern hier ihre Daten, um von jedem Ort aus, mobil oder stationär auf ihre Daten zugreifen zu können. Ein mehrstufiges Sicherheitssystem und viele Experten sorgen dafür, dass die Daten der Unternehmen sicher sind. „Tägliche Angriffe sind Normalität", weiß Stefanie Götz. „Wobei Angriff nicht gleich Angriff ist. Es gibt Angriffe, die schon so zur Normalität geworden sind, dass sie schon gar nicht mehr als Angriffe wahrgenommen werden. Die gezielten schweren Angriffe auf Netzwerke betreffen vor allem bekannte Unternehmen oder Institutionen. Die kleinen Angriffe, die ebenfalls großen Schaden anrichten können, kennt jeder: „Das sind zum Beispiel Spam- bzw. Betrugs-E-Mails, deren Ziel es ist, Daten abzugreifen", erklärt Stefanie Götz. „Aber auch diese können relevante wirtschaftliche Schäden verursachen, z.B. wenn die Unternehmens-IT aufgrund eines Verschlüsselungstrojaners komplett ausfällt und somit der Betrieb stillsteht. Dies hat man ja erst kürzlich mit Locky, Wannacry und Petya erlebt. Alle drei Viren haben sich beispiels-

weise auch über E-Mails via E-Mail-Anhänge in den Unternehmensnetzwerken verbreitet." Betriebe und sind sie noch so klein, brauchen einen umfangreicheren Schutz. Ein Virenscanner allein ist nicht ausreichend, erklärt Stefanie Götz. Der Schaden, der für Unternehmen entsteht, kann mitunter existenzgefährdend sein. „Wir sensibilisieren unsere Kunden stetig für diese Problematik. Und viele haben mittlerweile verstanden, dass es günstiger und um ein Vielfaches sicherer ist, die Daten in einer deutschen Cloud zu sichern, als im eigenen Betrieb", so Stefanie Götz.

Aus Spaß wurde Kriminalität

Zu Beginn des Siegeszuges des Internets stand vielen Programmierern von Viren und Würmern der Spaß im Vordergrund. Viele Hacker der ersten Stunde waren Tüftler und Computerenthusiasten, fasziniert von technischen Rätseln und der Herausforderung sich Zugang zu anderen System verschaffen zu können. Heute ist diese romantische Idee des Computer-Nerds nur noch eine Vorstellung aus vergangener Zeit. Das Programmieren und Verbreiten von Viren ist vor allem ein erfolgreiches Geschäftsmodell, das von organisierten kriminellen Banden beherrscht wird. Die zunehmende Professionalisierung dieser Banden und die Schlagzahl der aufeinanderfolgenden Angriffe verleihen dem Thema IT-Sicherheit seine Brisanz. Schließlich gilt: **Das ultimativ sichere Netzwerk gibt es nicht – wenn ein Hacker sich Zugang zu Ihren Daten verschaffen möchte, wird er dies auch schaffen.** Es ist nur eine Frage der Zeit und der Art und Weise. Das Gute ist, wie Stefanie Götz betont: „Je unbekannter ein Unternehmen, desto unwahrscheinlicher ist es, dass ein Hacker einen gezielten Angriff fährt. Doch Vorsicht: Es gibt zahlreiche Programme, die im Internet unzureichend geschützte Computer und Netzwerke ausspähen. Auch hier gilt: Gelegenheit macht Diebe!"

IT-Sicherheit bei BRZ

Mit einer Kombination aus organisatorischen und technischen Maßnahmen schützt BRZ die eigenen Daten und die seiner Kunden vor fremden und ungewollten Zugriffen. Die folgenden Maßnahmen stellen das Basis-Paket an IT-Sicherheit bei BRZ war. Je nach Gefährdungslage und individuellen Anforderungen der Kunden werden die Sicherheitsstrategien angepasst.

- Räumliche Zutrittskontrollen
- Zugangskontrollen zum Schutz vor Eindringung unbefugter Personen in das IT-System
- Zugriffskontrolle durch Berechtigungskonzepte, Protokollierung und Auditing
- Systeme zum Schutz der Daten vor Manipulation, Löschung und Diebstahl
- Sicherstellen der Verfügbarkeit der Daten durch
  - ein mehrstufiges Datensicherungskonzept
  - Viren- und Spamschutz
  - Firewall inkl. intelligentes Netzwerkeindringungssystem
  - Redundanz wichtiger Systeme und Infrastrukturkomponenten
  - Redundante Strom- und Kühlsysteme
  - Einsatz von Feuerschutzmaßnahmen

Weitere Infos: *www.brz.eu/de/fokus/it-sicherheit/*

Was bedeutet Angriff eigentlich?

„Definieren lässt sich ein Angriff als ein Versuch die Vertraulichkeit, Integrität oder Verfügbarkeit Ihrer Daten zu beeinträchtigen. Dies kann aus unterschiedlichen Gründen versucht werden. Die Ziele reichen von einem einfachen Diebstahl Ihrer Daten bis hin zu einem umfassenden Systemmissbrauch, wie der illegitimen Ressourcennutzung des Internets zum Spamversand.", erklärt Stefanie Götz.

Verbreitungswege von Viren und Co.

Viren, Würmer und Trojaner begegnen den Nutzern auf unterschiedlichen Wegen. „Ein klassischer Verbreitungsweg ist der E-Mail-Anhang", weiß die IT-Expertin. „Durch gefälschte Bewerbungen, Zahlungsanweisungen, Rechnungen oder Mahnungen werden Nutzer zu bestimmten Aktion oder einfach zum Herunterladen des E-Mail-Anhangs aufgefordert. Ein weiterer Verbreitungsweg ist das Surfen im Internet, hier reicht schon das öffnen bestimmter Webseiteninhalte, zur Einladung der ungebetenen Gäste aus", erklärt Stefanie Götz weiter. Ähnliches gilt für das Anschließen unbekannter Datenträger und die Installation unbekannter scheinbar harmloser Anwendungen. „Gerade im Unternehmen sollte man diese Dinge erst an einem Rechner ausprobieren, der nicht im Unternehmensnetzwerk eingebunden ist", erklärt Stefanie Götz. „Das Thema muss in jedem Unternehmen zur Chefsache werden!"

Iris Röder (M.A.),
BRZ Deutschland GmbH,
90425 Nürnberg