Die Gefahr aus dem Netz

Mit der fortschreitenden Digitalisierung wachsen auch die Sicherheitsanforderungen stetig – und überfordern viele Unternehmen. Holger May, Geschäftsführer der Tedesio GmbH aus Harburg, beantwortet die wichtigsten Fragen zum Thema Cybercrime.

Nehmen die Unternehmen die Gefahren aus dem Netz auf die leichte Schulter?
Definitiv ja. Es gibt nur zwei Arten von Unternehmen: die, die schon Opfer geworden sind, und die, die es noch nicht wissen. „Uns passiert schon nichts" ist leider noch oft das Motto vieler Unternehmen.

Welches sind die größten Sicherheitslücken?
Hier gibt es keine pauschalen Antworten, nur individuelle. Fakt ist, je digitaler unser Leben wird, um so offener stehen die Türen für Cyberkriminelle. Angriffspunkte sind beispielsweise technische und organisatorische Sicherheitslücken sowie nicht ausreichend geschultes Personal. Aber auch der Einsatz von Cloudlösungen verstärkt das Risiko. Durch die Implementierung von entsprechenden Prozessen kann dieses jedoch deutlich gemindert werden.

Gibt es Unternehmen, die anfälliger für Cybercrime sind als andere?
Ja. Wirtschaftskriminalität nimmt im unvorstellbaren Maß zu. So sind unter anderem Unternehmen mit eigener Produktentwicklung von höchstem Interesse sowie Finanzunternehmen und Klein- und Mittelständler mit eigenem Webshop und Internetauftritt.

Welche Anzeichen gibt es für einen Hack?
Die Anzeichen sind genauso unerschöpflich wie mögliche Sicherheitslücken: Leistungsverlust in der IT, eingeschränkte Erreichbarkeit des Unternehmens, der Verlust von Daten, defekte Datenbanken oder nicht erklärbare Veränderungen von Unternehmensdaten.

Fotos: StudiolinePhotography, shutterstock.com/vs148

Serie Digitale Welt

Die Digitalisierung ist ein Querschnittsthema, das alle Branchen betrifft: Vom papierlosen Büro über künstliche Intelligenz bis zu neuen Plattformen und Kommunikationskanälen – in der UW-Serie „Digitale Welt" beleuchten wir verschiedene Aspekte und geben praktische Tipps.

Der Experte

Holger May ist Geschäftsführer der Tedesio GmbH.

Was sollte ein Unternehmen tun, wenn es Opfer von Cybercrime geworden ist?
Melden Sie den Vorfall der Polizei. Durch ein Fachunternehmen wie die Tedesio wird die Feststellung der Schwachstelle und des Tathergangs mittels einer forensischen Untersuchung durchgeführt. Ergebnis sind Empfehlungen, die helfen, den Schaden zu minimieren oder in Zukunft zu vermeiden.

Warum versuchen Unternehmen häufig, ihr Sicherheitsproblem selbst zu lösen?
Ein Betrug oder die Manipulation von Unternehmensdaten wird häufig zu Unrecht als Versagen der eigenen IT Abteilung gesehen. Ein weiterer Punkt ist der angenommene Vertrauensverlust ihrer Kunden bei

Acht einfache Tipps zum Schutz der IT:

1. **Komplexe und unterschiedliche Passwörter nutzen**
2. **Vorsichtiger Umgang mit Anhängen oder Links in E-Mails von unbekannten Absendern**
3. **Datensicherung wöchentlich vornehmen**
4. **IT-Adminzugänge sparsam vergeben**
5. **Individuelle Mitarbeiterzugänge einrichten**
6. **Systemupdates und Sicherheitspatches schnell einspielen**
7. **Firmenserver mit Firewall sichern und diese auf dem neuesten Stand halten**
8. **Antivirenprogramm auf dem neuesten Stand halten**

Bekanntwerden des Vorfalls. Zusätzlich wird die Komplexität der Sicherheitslücke häufig unterschätzt.

Wie können sich Unternehmen im Vorfeld schützen? Gibt es eine wirkungsvolle Absicherung gegen Hackerangriffe?
Eine hundertprozentige Absicherung gibt es nicht. Jedoch reichen schon einfache Maßnahmen sowie technische Lösungen für eine deutliche Verbesserung des IT-Sicherheitsniveaus (siehe Tipps). Eine Sicherheitsbeurteilung mit Penetrationstest durch ein externes IT-Security-Unternehmen kann hier eine große Hilfestellung sein.

Wie teuer ist IT-Sicherheit?
Der richtige Mix aus IT-Lösungen und der Einhaltung von Sicherheitsregeln und Prozessen führt zu einer Gesamtlösung, die sich jedes Unternehmen leisten kann. Ein Sicherheitsvorfall, bei dem Kunden- oder Unternehmensdaten in falsche Hände geraten, ist in jedem Fall teurer. Übrigens unterstützt die Bundesregierung Unternehmen mit dem Programm „Go digital“. Gerne ist die Tedesio als autorisiertes Unternehmen bei der Beantragung der Mittel behilflich.

IT-Sprechtage

Kostenlose Sprechtage rund um das Thema IT-Sicherheit bietet unsere IHK regelmäßig an. Die nächsten Termine sind für Dienstag, 8. Oktober, von 10 bis 15 Uhr im Regionalbüro im ISI-Zentrum in Buchholz in der Nordheide und am Mittwoch, 23. Oktober, von 10 bis 15 Uhr in der IHK-Hauptgeschäftsstelle in Lüneburg geplant.
Anmeldungen bei Ute Jaster, jaster@lueneburg.ihk.de, Telefon 05361 2954-23.

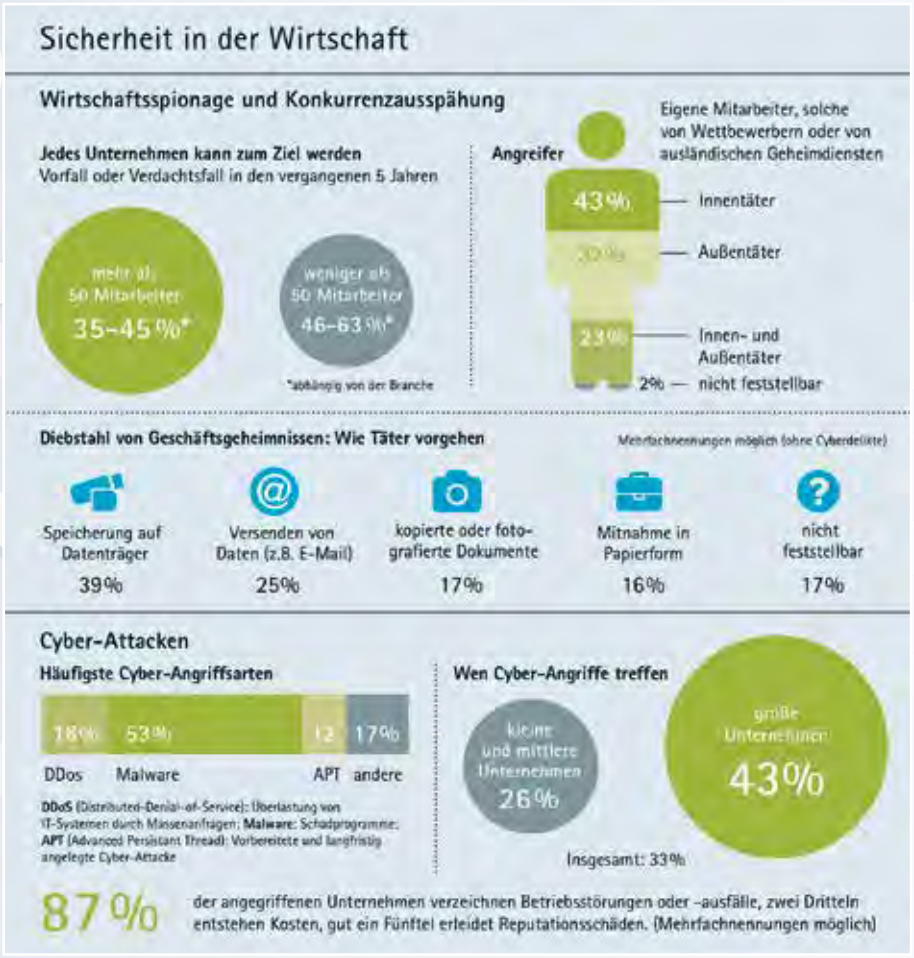
Praxisleitfaden zur Datensicherheit

Die Publikation „Datensicherheit – kurz und knapp“ informiert über die Methoden der Angreifer, über einen geeigneten Basisschutz und den grundsätzlichen Umgang mit Risiken. Der Ratgeber enthält auch eine Checkliste zum Handlungsbedarf, eine IT-Notfall-Karte, Links zu weiterführenden Informationen sowie ein Glossar. Er kostet 5,10 Euro zuzüglich Versand und kann per Mail bestellt werden beim DIHK-Verlag unter
bestellservice@verlag.dihk.de.

Wichtige Adressen für den Notfall

Bundesamt für Sicherheit in der Informationstechnik
Cyber-Sicherheit für die Wirtschaft
Godesberger Allee 185 -189
53175 Bonn
Telefon: 0228 99 9582-6254
E-Mail: frauke.greven@bsi.bund.de

Geschäftsstelle Allianz für Cyber-Sicherheit
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
Telefon: 0800 2741000
Fax: 022899 109582 6050
E-Mail: info@cyber-allianz.de
De-Mail: geschaeftsstelle-acs@bsi-bund.de-mail.de



Fotos: Leevke Struck, www.destinet.de, Donald Priebsch, Iris Lutzke; Quellen: WISKOS, BSI