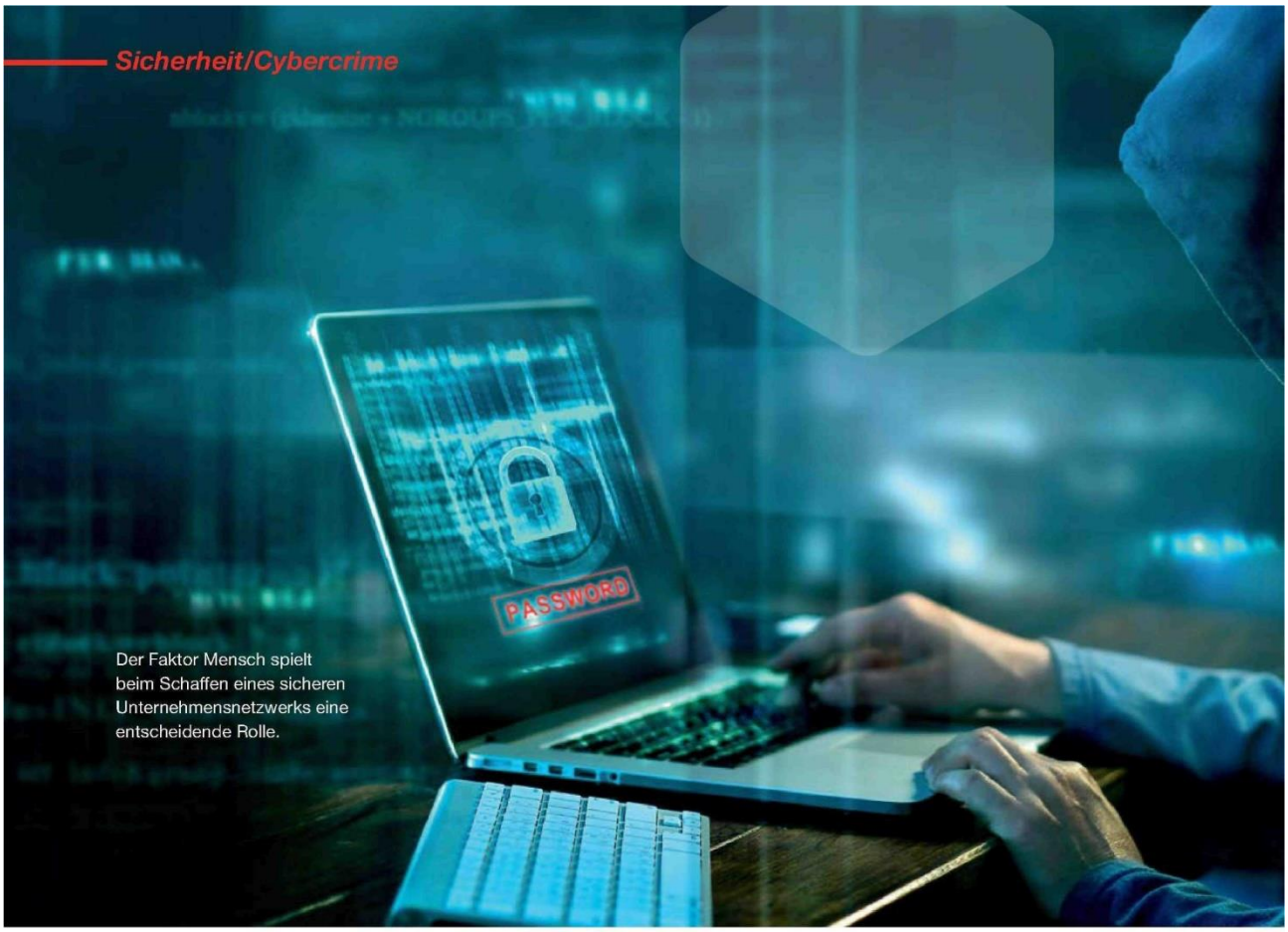

Der Faktor Mensch spielt beim Schaffen eines sicheren Unternehmensnetzwerks eine entscheidende Rolle.

ACHTUNG, Angriff!

7 Tipps, wie sich Unternehmen vor Cyberangriffen schützen können.

Angriffe auf die IT-Infrastruktur von Unternehmen sind in den letzten Jahren erheblich gestiegen. Mitverantwortlich dafür ist unter anderem die steigende Verbreitung von Ransomware durch E-Mails, Downloads sowie Sicherheitslücken in Browsern und Betriebssystemen. Mails, in denen Betrüger sich als Vorgesetzte ausgeben und Zahlungen oder die Herausgabe von Passwörtern anordnen – Stichwort Social Engineering –, sind ebenfalls immer öfter an der Tagesordnung. Eine weitere Cybercrime-Schiene, die die IT eines Unternehmens lahmlegt und dadurch oft enormen Schaden durch den Entgang von Einnahmen oder durch Reputationsverlust verursacht, sind Angriffe über sogenannte Botnets: Nicht erreichbare Websites und Webshops durch DDoS (Distributed-Denial-of-Service)-Attacken sowie durch Schadsoftware selbst zum Botnet-Zombie gemachte Rechner mit hohen Performanceverlusten zählen dazu. Die nachstehenden Tipps aus unserer Unternehmenspraxis sollen Sie im Kampf gegen Cybercrime unterstützen.

1. EFFIZIENTES PATCHMANAGEMENT

Ein effizientes Patchmanagement mit regelmässiger und zeitnaher Installation von Updates für die im Unternehmen eingesetzte Software, das Betriebssystem sowie das Antivirusprogramm und die Firewall sind einer der wichtigsten Schritte in Richtung IT-Sicherheit und Schutz vor Cybercrime. Idealerweise sollte dieser Punkt in jedem IT-Wartungsvertrag inkludiert sein. So wird sichergestellt, dass Unternehmen rasch wichtige Updates eingespielt bekommen und damit auf der sicheren Seite sind.

2. BEWUSSTSEIN BEI MITARBEITERN SCHÄRFEN

Meist wird Malware von Mitarbeitern durch unbedachtes Öffnen von E-Mail-Anhängen, Hyperlinks oder Dateien von externen Medien in das Unternehmensnetzwerk eingeschleust. Eine aktuelle Antivirus-Software bietet Schutz und

FOTOS: IPHOS, I-STOCK BY GETTY/IPOPBA

sollte selbstverständlich sein. 100%igen Schutz garantiert jedoch kein Programm. Der Faktor Mensch spielt beim Schaffen eines sicheren Unternehmensnetzwerks die entscheidendste Rolle. Mitarbeiter sollten daher über mögliche Gefahren aufgeklärt und im sicheren Umgang mit den Systemen geschult werden.

3. MIT DER RICHTIGEN BACKUP-STRATEGIE ZU BUSINESS-CONTINUITY

Hat man sich trotz Security-Massnahmen einen Verschlüsselungstrojaner eingefangen, sollte man besser auf eine umfassende Backup-Strategie – wie z. B. gespiegelte, sich gegenseitig überwachende Serversysteme und tägliche, offline aufbewahrte Sicherungen – gesetzt haben.

4. UNTERNEHMENSWEITE PASSWORTREGELUNG

Unsichere Passwörter wie einfache Zahlenkombinationen oder persönliche Informationen machen es Kriminellen leicht, ins Unternehmensnetzwerk einzudringen. Klare Vorgaben zur Passwort-Generierung und Aufbewahrung sowie die Verwendung unterschiedlicher Passwörter für unterschiedliche Anwendungen sorgen für einen besseren Schutz der Login-Daten. Wo es möglich ist, sollten Zugänge im Unternehmen mittels Zwei-Faktor-Authentifizierung geschützt sein.

5. GEMEINSAM MIT DEM ISP DDOS-ATTACKEN ABWEHREN

DDoS-Angriffe, bei denen mehr Datenverkehr auf bestimmte IP-Adressen umgeleitet wird, als diese verarbeiten können, richten sich im Allgemeinen gegen Web-, Mail- oder DNS-Server. Mit einer richtig konfigurierten Software sowie der passenden Dimensionierung der Infrastruktur kann man den Servercrash und Stillstand der IT-Infrastruktur verhindern. Die Zusammenarbeit mit dem Provider ist hier der wichtigste Schritt. Dieser kann den Datenverkehr im Backbone des Netzes überwachen und bei auffälligen Abweichungen nach oben sofort eingreifen.

6. INCIDENT-MANAGEMENT FÜR BUSINESS-CONTINUITY

Für eine optimale Business-Continuity ist Incident-Management mit einer Desaster-Recovery-Strategie von essenzieller Bedeutung. Das Wissen um die richtige Vorgehensweise ist oft über die Institution verstreut und in Ausnahmesituationen nicht effizient abzurufen. Zuvor festgelegte und getestete Prozesse können helfen, das Schlimmste zu verhindern und Folgeschäden zu minimieren.

7. OPTIMALES IT-RISKMANAGEMENT

Bei Cyberangriffen ist das Risiko hoch, dass auch sensible personenbezogene Daten im Unternehmen kompromittiert werden. Im Hinblick auf die im Mai in Kraft getretene DSGVO sollte eine Risiko-Analyse in Bezug auf die Unternehmens-IT nicht fehlen. Wenn dann trotz optimaler Sicherheitsvorkehrungen doch etwas passiert, ist man damit und mit den im Incident-Management festgelegten Strategien zur Schadensbegrenzung und -behebung abgesichert. ●

DER AUTOR

Ing. Christoph Wendl ist Gründer des 1998 ins Leben gerufenen IT-Unternehmens Iphos IT Solutions GmbH, das er gemeinsam mit Lyubomir Ivanov als Chief Executive Officer (CEO) leitet. In den 20 Jahren seines Bestehens ist Iphos zu einem internationalen Unternehmen mit Standorten in Österreich und Bulgarien angewachsen. Der Kundenkreis erstreckt sich auf den DACH-Raum sowie Bulgarien. Dabei nehmen sowohl internationale Konzerne wie KMU die Dienstleistungen von Iphos in den Bereichen IT-Infrastruktur, Softwareentwicklung und Webentwicklung in Anspruch.

Mehr Info: www.iphos.com