Digitalisierung Kleine und mittlere Unternehmen werden zunehmend Opfer von Betrug und Ransomware-Angriffen. Schützen Sie sich jetzt, um finanzielle Schäden zu vermeiden.

Sicher digitalisieren – grundlegende Cybersicherheit

Text: Gregor Wegberg | Foto: shutterstock.com

Längst werden kleine und mittlere Unternehmen von Cyberkriminellen ins Visier genommen. Täglich werden solche Unternehmen Opfer von Betrug und Ransomware-Angriffen – mit signifikanten finanziellen und personellen Folgen. Höchste Zeit also, dass sich auch Ihr Unternehmen schützt und auf dieses Geschäftsrisiko vorbereitet. Die drei grossen Risiken für Unternehmen sind Betrug, Missbrauch von Benutzerkonten und Ransomware. Sowohl im geschäftlichen als auch im privaten Bereich ist das sogenannte Phishing ein alltägliches Ärgernis. Unter Phishing versteht man die Betrugsmasche, unter Vortäuschung falscher Tatsachen an Kreditkartendaten oder Nutzerkonten zu gelangen. Eine Phishing-Website ist eine Kopie einer bekannten Website, um das Vertrauen der Kunden zu missbrauchen (z. B. Phishing-Website mit Logo der Post, um an Kreditkartendaten zu gelangen). Die Website-Adresse wurde hierzu per SMS und E-Mail verteilt. Eine finanziell besonders lukrative Form des Betrugs ist der CEO-Betrug und Rechnungsmanipulationsbetrug. Bei Ersterem geben sich Kriminelle als Geschäftsführer aus und bewegen Mitarbeiter dazu, einer Zahlungsaufforderung nachzukommen. Beim Letzteren verschaffen sich Cyberkriminelle Zugang zu den E-Mail-Konten ihrer Ge-

Die drei grossen Risiken für Unternehmen sind Betrug, Missbrauch von Benutzerkonten und Ransomware. Schützen Sie sich rechtzeitig davor und bringen Sie Ihr IT-System auf den neuesten Stand und kommunizieren Sie intern diese Thematik.

WISSEN

Um sich vor all diesen Gefahren aus dem Cyberraum zu schützen, muss zwingend zuerst auf folgende Schutzmassnahmen gesetzt werden:

- Setzen Sie Multi-Faktor-Authentifizierung, auch bekannt als Zwei-Faktor- oder zweistufige Verifizierung, für alle Benutzerkonten ein – insbesondere für alle aus dem Internet erreichbaren Dienste.
- Installieren und aktivieren Sie auf allen Computersystemen eine moderne Antivirenlösung. Sogenannte «Endpoint Detection and Response (EDR)»-Produkte sind zu bevorzugen.
- Setzen Sie eine Ransomware-resistente Datensicherungsstrategie (Backups) für alle Ihre Geschäftsdaten um. Hier ist besonders auf ein sogenanntes Write Once Read Many (WORM) oder Offline-Backup zu achten.
- Lassen Sie die Sperrlisten aktivieren, damit keine bekanntlich schädlichen Internetadressen besucht werden können. Dies ist besonders einfach, wenn ein DNS-Dienst wie Quad9 auf allen Computern eingerichtet und genutzt wird.
- Halten Sie alle Ihre IT-Systeme auf dem aktuellen Stand und spielen Sie Updates zeitnah ein. Dies gilt speziell für alle Systeme, die aus dem Internet erreichbar sind.
- Sensibilisieren Sie Ihr Personal. Dazu gibt es verschiedene kostenpflichtige Produkte und kostenlose Ressourcen. Ein regelmässiger Austausch zu aktuellen Gefahren mit den Mitarbeiterinnen und Mitarbeitern hält das Bewusstsein hoch.
- Zahlungen sollten nur auf bereits bekannte Bankkonten oder bloss nach telefonischer Rücksprache mit der verantwortlichen Person zur Überprüfung des Empfängerkontos erfolgen.

INFO

Schützen Sie Ihr KMU

Weitere Informationen zu Schutzmassnahmen finden Sie beim Bundesamt für Cybersicherheit BACS.

ncsc.admin.ch

schäftspartner und senden unter einem Vorwand manipulierte Rechnungen mit geänderter IBAN zu. Beide Betrugsmaschen führen dazu, dass Geld an die Kriminellen überwiesen wird. Neben Ransomware gehören diese Formen des Betrugs zu den finanziell schädlichsten für Unternehmen.

In aller Munde: Ransomware

Ursprünglich handelte es sich bei Ransomware um Schadprogramme, die Unternehmensdaten verschlüsseln und nur gegen Zahlung eines Lösegelds (engl. Ransom) wieder zugänglich machen. Moderne Ransomware-Angriffe gehen einen Schritt weiter. Damit ein Opfer der Lösegeldforderung und Erpressung nachkommt, stehlen die Cyberkriminellen Daten und drohen, sie zu veröffentlichen, verschlüsseln Geschäftsdaten, um den normalen Geschäftsbetrieb zu unterbrechen, und zerstören Datensicherungen, um eine schnelle Rückkehr in den Normalbetrieb zu verhindern.

Neue Norm – nur eine Frage der Zeit

Alle unten genannten und weitergehenden Schutzmassnahmen bieten keinen perfekten Schutz. Diesen gibt es in der Cybersicherheit nicht. Deshalb muss man heute davon ausgehen, dass man zwangsläufig betroffen sein wird. Es lohnt sich daher, die folgenden zwei Schritte vorzubereiten und im Ernstfall auszuführen:

- Alle IT-Systeme vom Internet trennen. Dies verhindert, dass Cyberkriminelle weiterhin Zugriff auf Ihre Daten und Systeme haben.
- Rechtzeitig Experten hinzuziehen, um eine effiziente und sichere Rückkehr zum Normalbetrieb zu gewährleisten. Zumindest sollte die Notfallnummer eines Computer Security Incident Response Teams (CSIRT) notiert werden, um dieses rechtzeitig zur Unterstützung hinzuzuziehen.

ONECONSULT.COM

PORTRÄT

© ZVG

Gregor Wegberg
Head of Digital Forensics & Incident Response
Member of the Management Board
Oneconsult AG

Oneconsult ist ein Schweizer Cybersecurity-Services-Partner, der seit 2003 tätig ist. Mit Büros in Zürich, Bern, München und Auckland bietet das Unternehmen eine Vielzahl von Dienstleistungen wie Red Teaming, Penetration Testing und Incident Response an. Das Team steht für gründliche Sicherheitsanalysen, massgeschneiderte Präventionsmassnahmen und schnelle Reaktionen auf Cyberattacken. Mit ihrem internationalen «Computer Security Incident Response»-Team sind sie rund um die Uhr verfügbar und unterstützen Organisationen aus verschiedenen Branchen bei allen Cybersecurity-Themen.