IT-Sicherheit: 7 Tipps für Unternehmen und öffentliche Einrichtungen

Weltweit haben sich die Informations- und Netzwerktechnologien rasant weiterentwickelt und damit die Verhaltensweisen der Menschen sowie die Arbeits- und Geschäftsprozesse verändert. Das Internet und seine Möglichkeiten sind aus Wirtschaft und Gesellschaft nicht mehr wegzudenken. Gleichzeitig werden aber auch immer mehr Bürgerinnen und Bürger, aber auch Unternehmen und öffentliche Einrichtungen Opfer von Cybercrime. Das Bundeskriminalamt informiert und gibt Tipps, wie sie sich davor schützen können.

1. Schulung und Sensibilisierung

Zur Vorbeugung von Bedrohungen und zur Reduzierung von Risiken leistet das Mittel der Mitarbeiterschulung den größten und wirkungsvollsten Beitrag. Aufmerksamkeit und kritisches Hinterfragen im Tagesgeschäft ist ebenfalls von äußerster Bedeutung. Gegenseitige Kontrolle besonders bei sicherheitsrelevanten Handlungen kann Fehler aufzeigen und abwenden.

2. Zugriffsschutz

Passwörter sollten nicht notiert und stets geheim gehalten werden sowie einer zuvor festgelegte Richtlinien entsprechen. Ein gutes Passwort besteht in der Regel aus mindestens acht Zeichen, wobei diese Zeichenfolge aus Zahlen, Buchstaben und Sonderzeichen bestehen muss, um einfachen Wörterbuchattacken standhalten zu können. Regelmäßiges Ändern eines Passworts hebt das Sicherheitsniveau zusätzlich. Geräte, denen durch den Hersteller ein Standard-Passwort vergeben wurde, sind mit einem neuen Passwort zu versehen, da diese durch den Hersteller vorgegebenen Passwörter meist öffentlich bekannt sind.

3. Wireless LAN (WLAN)

In den Einstellungen eines WLAN-Routers ist es notwendig den Verschlüsselungsstandard WPA oder WPA-2 zu wählen. Sollte das Gerät nicht über eine dieser Einstellungen verfügen, ist wenigstens der unsichere Standard WEP zu verwenden. Bei der Konfiguration eines WLANs ist darauf zu achten, dass Standard-Schlüssel die durch den Hersteller vorgegeben wurden, durch einen eigenen geheimen Schlüssel ersetzt werden. Die Bezeichnung der sogenannten SSID ist neutral zu vergeben, damit das Drahtlosnetzwerk einer bestimmten Einrichtung von außerhalb nicht zugeordnet werden kann.

4. Sicherheitssoftware

Anti-Viren Programme und Firewalls können einen Computer bzw. ein Netzwerk nur dann schützen, wenn diese Programme durch regelmäßige Updates gepflegt werden. Dies betrifft grundsätzlich auch alle anderen Programme, die auf einem Computer installiert wurden, damit bekannte Sicherheitslücken geschlossen werden können.

5. Schutz sensibler Daten

Auf externen Datenträgern (USB-Sticks, externen Festplatten, DVDs usw.) dürfen keine Daten unverschlüsselt gespeichert werden, die nicht für die Öffentlichkeit bestimmt sind. Beim Verlassen des Arbeitsbereichs kann durch gleichzeitiges Betätigen der Tasten „Windows-Taste+L“ ein Computer mit Windows-Betriebssystem gesperrt werden, Papierdokumente und Datenträger sind bei längerer Abwesenheit vom Arbeitsbereich ebenfalls zu entfernen.

6. Sichere Webseiten

Die Preisgabe von internen Informationen auf Webportalen oder Informationen durch aussagekräftige Fehlermeldungen auf Webseiten im Falle eines Systemfehlers verschaffen Angreifern wesentliche Vorteile. Versionsnummern von Softwareprodukten, der Herstellername der Software sowie aussagekräftige Fehlermeldungen (Angabe der fehlerhaften Datei oder des Speicherorts der Datei) sind Informationen, die es zu schützen gilt. Alle vertraulichen Informationen auf Webservern sind in ein passwortgeschütztes Verzeichnis abzulegen. Damit bestimmte Verzeichnisse bzw. Passwortdateien nicht über eine Suchmaschine gefunden werden können, kann eine „robots.txt“ im Stammverzeichnis des Webservers verwendet werden. Falls kein Zugriff zum Stammverzeichnis erfolgen kann, sind „Meta-Tags“ (<meta name="robots" content="noindex">) im „Header“ der Webseite hilfreich.

7. Social Engineering

Der erste Schritt eines Hackers beginnt mit dem Ausforschen von Informationen. Diese Informationen erlangen Angreifer meist durch Anrufe mit gefälschter Identität oder durch die persönliche Begehung des Geschäftsbereichs. Nützliche Informationen befinden sich oftmals in Mülltonnen in denen (DVDs, CDs, Post-its) oder Ausdrucke mit firmeninterner Informationen vollständig enthalten sind. Papierdokumente oder Datenträger sind daher vor der Entsorgung fachgerecht durch entsprechende mechanische Verfahren zu vernichten.

Verdächtige Sachverhalte im Internet melden Sie bitte an die Internetmeldestelle im Bundeskriminalamt against-cybercrime@bmi.gv.at.

Weitere Information erhalten Sie auf der nächsten Polizeiinspektion, auf der Homepage www.bmi.gv.at/praevention und neuerdings auch per BM.I-Sicherheitsapp.

Die Spezialisten der Kriminalprävention stehen Ihnen kostenlos und österreichweit unter der Telefonnummer 059133 zur Verfügung.