handwerk. magazin

www.handwerk-magazin.de

Anleitung:

IT - SICHERUNG

Autor: **Frank Pollack**, freier Journalist

IMMER AUF DER SICHEREN SEITE

IT - SICHERHEIT

Jürgen Schüler, Leiter des Zentrums für IT- Sicherheit (KOMZET) in Mainz, berät seit vielen Jahren Handwerksbetriebe bei der Vorsorge gegen Cyberkriminalität. Die wichtigsten Eckpunkte für ein Sicherheitskonzept hat er in der folgenden Checkliste zusammengefasst.

LEITLINIEN. Sie regeln den sicheren Umgang mit der Informationstechnik im Unternehmen, wie zum Beispiel: Wer darf auf welche Programme, welche Geräte und Daten zugreifen? Unter welchen Voraussetzungen dürfen fremde Datenträger angeschlossen werden? Wie müssen Passwörter beschaffen sein? Die Leitlinien müssen regelmäßig angepasst und in Soft- und Hardware (zum Beispiel mit Zugangsberechtigungen) umgesetzt werden.

SENSIBILISIERUNG. Kommunizieren Sie die IT-Sicherheitsleitlinien aktiv. Zeigen Sie, dass leichtfertiger Umgang zum Beispiel mit E-Mails (siehe Kasten auf Seite 42) Arbeitsplätze und sogar die Existenz des gesamten Unternehmens gefährden kann. Verdeutlichen Sie Ihren Mitarbeitern den Wert von Passwörtern, von Informationen auf Firmenrechnern und Mobilgeräten! Gewinnen Sie die Mitarbeiter dafür, selbst Schwachstellen aufzudecken und zu beseitigen.

BAULICHE SICHERHEIT. Der Server und andere wichtige Geräte des Firmennetzwerkes sollten in einem Raum untergebracht sein, der für Besucher unzugänglich und auch gegen Einbruch besonders gesichert ist. Sorgen Sie gegen Energieausfälle vor, zum Beispiel mit einer unabhängigen Stromversorgung. Achten Sie darauf, dass Router, Netzwerkleitungen und Schaltkästen nicht außerhalb der Firmenräume installiert wurden.

UPDATES. Die gesamte Software des Unternehmens, allen voran Betriebssysteme, E-Mail-Programme, Browser und Office-Pakete, müssen stets auf dem neuesten Stand gehalten werden. Benennen Sie Verantwortliche für Neuinstallationen und Updates namentlich.

VIREN- UND MALWARESCHUTZ. Eine stets aktuelle Antiviren-Software mit Malwareerkennung ist Grundvoraussetzung für sicheres Arbeiten im Netz. Beachten Sie, dass auch mobile Geräte wie Smartphones und Tablets mit abgesichert werden. Professionelle Vergleichstests zeigen, welche Schutzwirkung die verschiedenen Pakete in der Praxis haben und wie nutzerfreundlich sie sind.

GERÄTESICHERHEIT. Halten Sie die Firmware für Internetrouter, Telefonanlagen, Drucker und andere vernetzte Geräte stets auf aktuellem Stand. Entscheiden Sie sich bei Neuanschaffungen bevorzugt für Geräte von Herstellern, die aktive Produktpflege in Form von Updates betreiben. Ersetzen Sie vom Hersteller voreingestellte Codes oder Passwörter durch eigene. Nutzen Sie für Tablets und Smartphones Mobile-Device-Management-Systeme (MDM), mit denen deren Sicherheitsfunktionen und Updates zentral gesteuert werden können.

BACKUP. Sorgen Sie für regelmäßige Datensicherungen aller wichtigen Laufwerke. Achten Sie darauf, dass mindestens ein vollständiges und möglichst aktuelles Backup vom Firmennetz getrennt aufbewahrt wird, um eine Verschlüsselung durch eingedrungene Schadprogramme zu verhindern. Testen Sie regelmäßig, ob die Backups auch funktionstüchtig sind. Denn Fehler kommen bei Datensicherungen häufiger vor, als die meisten Anwender vermuten

IT - SICHERHEIT

So entlarven Sie gefährliche E-Mails:

Die E-Mail ist Hackers Liebling. In drei von vier Fällen nutzen Cyberkriminelle elektronische Nachrichten für ihre Angriffe. Timo Gehle, Leiter Consulting für IT-Sicherheit und IT-Strategie der DATEV in Nürnberg, erklärt, wie Sie gefährliche Nachrichten rechtzeitig erkennen.

ABSENDER. Kennen Sie den Versender? Stellt er Kontaktdaten zur Verfügung und sind diese verifizierbar? (Nicht auf Links klicken, siehe Punkt 3!) Erwarten Sie eine Nachricht von ihm und ist der Anlass plausibel? Selbst wenn alle Fragen mit Ja beantwortet werden können: Bleiben Sie misstrauisch. Denn Kriminelle tarnen sich gern mit bekannten Namen, etwa von Telefonanbietern oder Online-Shops. Sogar die Identität von Freunden oder Geschäftspartnern anzunehmen ist für sie mit ein paar Recherchen im Netz kein Problem.

INHALT. Passen Aussagen und Tatsachen zusammen? Wenn der Betreff zum Beispiel „Ihre Bestellung“ lautet, Sie bei dem vermeintlichen Absender aber lange Zeit nichts gekauft haben, ist Vorsicht angesagt. Ebenso wenn versucht wird, Druck aufzubauen, etwa mit relativ unbestimmten Formulierungen wie „Rechnung“ oder „Inkasso“ ohne Nennung einer für Sie nachprüfbaren Vorgangsnummer. Oder wenn Inhalt und Stil des Geschriebenen widersprüchlich erscheinen (ein vertrauter Geschäftspartner Sie zum Beispiel mit „Sehr geehrte Damen und Herren“ anspricht).

VERLINKUNGEN. Klicken Sie nie auf Links, deren Herkunft und Ziel Sie nicht hundertprozentig kennen! Links können zu anderen Adressen führen, als sie nach außen anzeigen. Das gilt auch für E-Mail-Adressen. Geben Sie Adressen deshalb besser von Hand ein (zum Beispiel in ihren Browser), statt auf Links zu klicken. Wenn Sie aufgefordert werden, Passwörter zu ändern, ohne dass Sie das selbst veranlasst haben, sollten Sie dem keinesfalls Folge leisten!

ANHÄNGE. In angehängten Dateien wird Schadsoftware besonders häufig versteckt. Größte Vorsicht ist geboten bei Anhängen mit den Endungen .exe, .vbs, .js, .com oder .bat. Aber selbst Word-Dokumente, Excel-Tabellen, PDFs oder Bilder (.jpg) können einen ausführbaren Code enthalten. Klicken Sie deshalb nur auf Anhänge, die Sie erwarten und deren Absender Sie sicher kennen! Stellen Sie Ihr Mailprogramm (zum Beispiel Outlook) so ein, dass Bilder und Anhänge nicht automatisch heruntergeladen werden.

Wichtig. Bleibt nach diesen Prüfschritten auch nur ansatzweise ein ungutes Gefühl, sollten Sie die Mail weder anklicken noch öffnen. Gelingt es nicht, Herkunft und Inhalt der Nachricht auf unabhängigem Weg (zum Beispiel über eine Telefonnummer) zu überprüfen, bleibt nur eines: löschen.