01.12.2017

IT-Sicherheit von E-Mail bis Smartphone

Referenten zeigen im IHK-Tagungszentrum, wie Unternehmen ihre Daten schützen sollten

Geraten Kundendaten in falsche Hände, kann das für Unternehmen nicht nur teuer werden, es kratzt auch an ihrem Renommee. Die Nutzung mobiler Endgeräte erhöht die Zahl der Einfallstore für Sicherheitsangriffe zusätzlich. Deshalb haben die IHK und die Handwerkskammer Trier sechs Referenten zu ihrem IT-Sicherheitstag eingeladen, um Unternehmen Tipps zum Schutz ihrer Daten zu geben.

Dass kleine und mittlere Unternehmen die Sicherheit ihrer IT oft stiefmütterlich behandeln, ist laut Michael Weirich, Security Analyst bei „eco – Verband der Internetwirtschaft“, das Kernproblem. „Oft investieren sie nicht proaktiv, sondern reaktiv, also wenn der Schaden bereits entstanden ist.“ Dabei verursachten Cyberangriffe allein mit der Verletzung von Geschäfts- und Betriebsgeheimnissen einen Schaden von schätzungsweise 609 000 Euro pro Vorfall.

Schon einfache Mittel helfen

Das schwächste Glied seien die Mitarbeiter, die täglich mit dem Internet arbeiten, aber nicht internetaffin seien – also beispielsweise die Buchhaltung, die mit gefälschten Rechnungen konfrontiert werde. Phishing-Mails würden immer professioneller und damit ein ideales Einfallstor für Viren und Trojaner. Aufgrund der zunehmenden Vernetzung könnten inzwischen selbst Kühlschränke und Fernsehgeräte mit Viren infiziert sein.

„Die meisten Infektionen lassen sich aber mit einfachsten Mitteln verhindern“, sagt Weich. Seine Tipps:

- Anti-Virenprogramme, Spam-Filter, Ad-Blocker und kontinuierlich Updates installieren
- keine E-Mail-Anhänge von unbekannten Absendern öffnen (oder nur in einer gesicherten virtuellen Umgebung)
- sichere Passwörter nutzen
- regelmäßig die Daten sichern
- keine persönlichen Daten (Bankkarte, Führerschein et cetera) in das Internet eingeben
- unsichere WLANs meiden, insbesondere öffentliche Hotspots
- kostenlose Dienste nutzen, die die eigenen Accounts überwachen und im Fall eines Datendiebstahls eine Nachricht schicken
- den Ernstfall mit „digitalen Feuerübungen“ proben
- Mitarbeiter schulen und sensibilisieren
- IT-Sicherheit zur Chefsache machen.

Nicht erpressen lassen!

Werde man zu einer Geldzahlung aufgefordert, weil ein Erpressungstrojaner den Zugang zu den Daten verhindere, solle man darauf in keinem Fall eingehen. Verlaufe die Suche nach einer entsprechenden Entschlüsselungssoftware erfolglos, solle der Betroffene die Daten aus dem Backup zurückinstallieren.

Die Webseite sei wegen Sicherheitslücken in Standardprogrammen anfällig für Cyberangriffe. Meist dauere es dann zu lange, bis die Webseiten-Betreiber mit Updates reagieren. Mit „Siwecos“ habe man einen kostenlosen Dienst für KMU entwickelt, um Sicherheitslücken auf ihren Webseiten zu erkennen und zu beheben.

Herausforderung mobile Endgeräte

Mobile Endgeräte würden inzwischen wie PCs genutzt, seien aber selten mit Anti-Viren-Programmen ausgestattet, so Weirich. Wo bei der Nutzung von Smartphones, Tablets et cetera Fallen lauern, erläuterte Professor Konstantin Knorr vom Fachbereich Informatik der Hochschule Trier.

Zum einen könne man die Geräte leichter verlieren, was eine Festplatten-Verschlüsselung erforderlich mache. Passwörter von Smartphones ließen sich leichter ausspähen, die Hardware sei schwächer, die Bandbreite geringer. Zudem seien für „ältere“ Geräte schnell keine Updates mehr verfügbar. Kabellose Funknetze seien leichter angreifbar und die Angreifer schwerer zu lokalisieren. Personenbezogene Daten und biometrische Merkmale könnten per Smartphone leichter erfasst und abgegriffen werden.

Für die neue EU-Datenschutz-Grundverordnung sensibilisierte anschließend Christoph Preetz vom Security-Hersteller ESET die Zuhörer. Sie löst ab dem 25. Mai 2018 bisherige nationale Regelungen ab. Da es keine Übergangsfrist gebe, müssten Unternehmen schon jetzt die nötigen Vorkehrungen treffen. Die IHK informiert darüber am 5. Februar 2018 in einer separaten Veranstaltung.

Über die Sicherheit und Transparenz im Netzwerk durch die Netzwerkszugangskontrolle NAC sprach auf dem IT-Sicherheitstag Christopher Marvin Eißner von der macmon secure GmbH (Berlin). Harald Beutlhauser (Rohde und Schwarz Cybersecurity, München) informierte über den Schutz webbasierter Applikationen, und Alexander Dörsam (Antago GmbH, Heppenheim) demonstrierte ein Live-Hacking.