Cyberkriminalität bedroht den Mittelstand

Es steht viel auf dem Spiel

Datendiebstahl ist im zweiten Jahrzehnt des 21. Jahrhunderts zu einem der dringlichsten Sicherheitsprobleme erwachsen. Innerhalb der letzten zwei Jahre sind weltweit nahezu ein Viertel aller Firmen Opfer von Cyberkriminalität geworden.

Cyberkriminalität ist also auch in Deutschland real existierend. Besorgt scheinen aber längst nicht alle deutschen Unternehmen zu sein. Gerade bei den Mittelständlern scheint das Risikobewusstsein im Hinblick auf die Cyberkriminalität noch keineswegs ausgeprägt zu sein. Die innerhalb einer Studie ermittelten Zahlen sind jedenfalls in der Tat besorgniserregend. Demnach sehen gerade einmal neun Prozent aller befragten Betriebe die eigene Datensicherheit als bedroht an. Dieser geringe Prozentsatz verwundert nicht nur, die Sorglosigkeit vieler mittelständischer Unternehmen kann sich zudem bitter rächen. Wenn sie nämlich auf ihre Versicherung setzen, könnten sie enttäuscht werden. Die so bezeichneten Vertrauensschadensversicherungen oder auch die klassischen Elektronikversicherungen decken IT-spezifische Gefahren wie eben Cyberangriffe lediglich bedingt bzw. nur in einzelnen Teilbereichen ab.

Herkömmliche Versicherungen decken Schäden aus Cyberangriffen unzureichend ab. Wenn überhaupt, können sich die mittelständischen Unternehmen adäquat mittels einer Cyberversicherung schützen. Zwar hält eine Versicherung dieser Art nicht einen Täter von einem digitalen Angriff ab, aber zumindest die finanziellen Folgen einer solchen Attacke können abgefedert werden. Trotzdem kann jede einzelne kriminelle Attacke auf die Computersysteme und Netzwerke eines Unternehmens fatale Folgen haben. Ein durch den Datenklau einhergehender Image- und Vertrauensverlust kann sogar zu existentiellen Problemen ausufern. Zudem können Hackerangriffe ein Unternehmen für eine gewisse Zeit komplett lahm legen. Viele Unternehmen sind nämlich auf eine sowohl funktionierende als auch funktionelle Technik angewiesen; die Digitalisierung der Daten schreitet schließlich unentwegt voran. Fällt die Technik aus und hat das Unternehmen dann auch keinen direkten Zugriff auf Daten und Zahlen, kann prompt die Zukunft eines Betriebes auf dem Spiel stehen.

Johannes Müller von der Johannes Müller Wirtschaftsberatung (BDU) Finanzkommunikation und Unternehmenssteuerung

Bei der Komplexität des Themas Cyberkriminalität ist es aber auf jeden Fall ratsam ein kompetentes Beratungsunternehmen einzubinden. Unabhängige IT-Spezialisten helfen Schwachstellen und Risiken in den betrieblichen EDV Systemen sowie im betrieblichen Umgang mit der IT-Technik zu identifizieren. ■

■ Weitere Informationen:
www.mueller-beratung.de

Digitalisierung der Wirtschaft /Industrie 4.0

Große Herausforderung an die IT-Sicherheit

Die Digitalisierung als Innovationsmotor unserer Unternehmen bietet die Chance, dem globalen Wettbewerb ein Stück voraus zu sein. Dabei werden sich Wertschöpfungsketten ändern und neue Geschäftsmodelle entstehen.

Bereits heute gibt es Plattformen, die unterschiedliche Maschinen miteinander „sprechen" lassen - Experten reden hier vom „Internet der Dinge". Dies sorgt für unmittelbaren Nutzen: So lassen sich zum Beispiel Maschinen deutlich besser auslasten, die Fertigung unterschiedlicher Produkte kann automatisch dem Bestelleingang folgen. Maschinen können durch diese Technologie freie Kapazitäten „ins Netz" melden – die intelligente Steuerung sorgt für eine höhere Auslastung. Auch die laufende Überwachung sowie die Meldung und weitgehend automatisierte Beseitigung von Störungen werden stark vereinfacht.

Für Unternehmen ist es zwingend erforderlich, sich mit diesem Themenkomplex zu beschäftigen. Denn die Vernetzung der Produktion ist eine zentrale Zukunftschance der Digitalisierung. Damit steigen auch die Anforderungen an die Sicherheit der Systeme. Durch die Digitalisierung überträgt sich die wachsende Bedrohung von IT-Systemen durch Cyberangriffe automatisch auch auf industrielle Anlagen. Der jährliche finanzielle Schaden durch Industriespionage beläuft sich laut einer Studie von Corporate Trust in Deutschland auf 11,8 Milliarden Euro.

Die Verbreitung der Datenübertragung über WLAN nimmt stetig zu. Und damit auch die Sicherheitsanforderungen. Im privaten oder beruflichen Umfeld kommt für die Anmeldung und Authentifizierung am WLAN in der Regel nur ein einziger, vorab verteilter Netzwerkschlüssel zum Einsatz – Pre-Shared Key (PSK) genannt. „Im Internet der Dinge kommt man nicht umhin, die Maschinen durch individuelle Schlüssel abzusichern. Die jeweiligen Zugriffe auf die Systeme werden so auf ihre Funktionen beschränkt. Dazu ist es notwendig, für ein übergreifendes Management der Systeme zu sorgen und die Aktivitäten der Geräte zu überwachen", beschreibt Andreas Tracz, Geschäftsführer der K&K Networks GmbH. Sollte zum Beispiel eine „smarte" Glühbirne versuchen,

Andreas Tracz, Geschäftsführer der K&K Networks GmbH: „Durch die Digitalisierung überträgt sich die wachsende Bedrohung von IT-Systemen durch Cyberangriffe automatisch auch auf industrielle Anlagen."

auf die Personalakten zuzugreifen, wisse der Systemadministrator sofort, dass etwas nicht stimme.

Ein Angreifer kann die Sicherheitstechnik einer Glühbirne also möglicherweise kompromittieren, kommt danach aber nicht weiter, da deren Zugriffsrechte auf eine Aktion wie „Licht an / Licht aus" beschränkt sind. Der Schaden für ein Unternehmen bleibt in diesem Falle selbst bei einem erfolgreichen Angriff begrenzt.

Voraussetzung hierfür ist eine professionelle WLAN-Sicherheitsstrategie in Zusammenspiel mit der Firewalltechnologie. Hierzu gibt es verschiedene Ansätze von unterschiedlichen IT-Dienstleistern. Zum Beispiel bietet die K&K Networks GmbH unter dem Namen „Secure Access Service" passfähige Security Pakete für die Anforderungen im Mittelstand an und sorgt damit für umfassende Unternehmenssicherheit – auch im „Internet der Dinge" beziehungsweise für die Industrie 4.0. ■

■ Weitere Informationen: www.kuk-networks.de

BREKOM

WLAN-Performance für kabellose Unternehmen

BREKOM setzt in der WLAN-Performance einen weiteren Impuls: Der Over-the-Air Quality of Service mit konvergentem Sprach- und Daten-Service erfolgt über eine einzige WLAN-Infrastruktur.

Heutzutage muss ein Unternehmensnetzwerk performanter sein als je zuvor. Mitarbeiter bringen ihre eigenen Endgeräte mit (Stichwort „Bring Your Own Device" – BYOD) und erwarten konstante Verbindungen sowie eine hohe Netzwerkperformance. Die WLAN-Experten des regionalen Dienstleisters BREKOM setzen leistungsfähige Produkte des Herstellers Meru ein, um es IT-Managern zu ermöglichen, die Anforderungen moderner WLAN-Umgebungen mit