Digitale Welt

So verändert Digitalisierung unsere Wirtschaft

Die Online-Spione lauern überall

Gehackte Rechner, abgehörte Anrufe, mitgelesene Mails – für Firmen wird es immer schwerer, sich vor Angriffen zu schützen.

Unser Leser
Dirk Volkmann
aus Königslutter fragt:

Wie ist das Mithören von Telefonaten und das Mitlesen von E-Mails rechtlich zu bewerten?

Die Antwort recherchierte
Daniel Freudenreich

Auch der Deutsche Bundestag ist vor Cyber-Kriminalität nicht sicher: Vor wenigen Tagen wurde bekannt, dass Unbekannte mit einem Trojaner regelmäßig vertrauliche Dateien von den Rechnern der Parteien ausspähen. Foto: dpa

Sogar das Handy von Bundeskanzlerin Angela Merkel wurde ausspioniert. Archiv-Foto: Michael Kappeler/dpa

Experten raten davon ab, sensible Daten auf Cloud-Diensten wie Dropbox zu lagern. Archiv-Foto: Armin Weigel/dpa

Ebay-Nutzer sollten nach einem Hackerangriff 2014 ihre Passwörter Wechseln. Archiv-Foto: Inga Kjer/dpa

Braunschweig. Sebastian Brandes, den Chef der Salzgitter Maschinenbau AG (SMAG), hatte schon länger ein ungutes Gefühl beschlichen. Denn der Internet-Verkehr zwischen dem Hauptsitz in Salzgitter und den Tochtergesellschaften in China sei „sehr langsam“ gewesen.

Schließlich beschloss die SMAG, der Ursache auf den Grund zu gehen – und erlebte eine üble Überraschung. „Durch eine interne Analyse konnten wir feststellen, dass unser System überwacht und unsere Mails mitgelesen werden“, erzählt Brandes und meint: „Es ist unheimlich schwer, sich dagegen erfolgreich zur Wehr zu setzen.“

Ja, vor Jahrzehnten war der Schutz von Betriebsgeheimnissen noch eine recht simple Sache. Oft reichten stabile Türen, ein Sicherheitsdienst und der Tresor hinter dem Ölgemälde. Doch spätestens seit Edward Snowden weiß auch die breite Öffentlichkeit, dass die Bedrohung in Zeiten der Digitalisierung heute ganz anders aussieht. Wer telefoniert oder skypet, kann mit etwas krimineller Energie problemlos belauscht werden. Hacker können von jedem Winkel der Erde aus E-Mails mitlesen und Firmennetzwerke knacken, wenn diese nicht ausreichend gesichert sind. Trojaner, Viren und Spionage-Programme sorgen für immer größere Bedrohungen für Firmen. Dazu ein Überblick:

Hackerangriffe verdoppelt

Verfassungsschützer gehen davon aus, dass den deutschen Unternehmen jährlich ein Schaden von 50 Milliarden Euro durch Hacker-Attacken entsteht. Alle drei Minuten sollen sich Wirtschaftsspione, vor allem aus China, in deren Rechner einschleichen.

Nicht von ungefähr fürchten 76 Prozent der Betriebe einen Angriff aus dem Netz, wie aus einer Umfrage des Sicherheits-Software-Anbieters G-Data von 2014 hervorgeht. Dass diese Sorge berechtigt ist, unterstreicht das Landeskriminalamt Niedersachsen. So hat sich die Zahl der Hackerangriffe auf niedersächsische Firmen fast verdoppelt. Während das LKA 2013 lediglich 60 Fälle von Computer-Sabotage registrierte, waren es 2014 bereits 110. Das ist wohl nur die Spitze des Eisbergs. Häufig scheuen sich Unternehmen, Anzeige zu erstatten, wie die Behörde berichtet.

„Auch die höchsten Sicherheitsstandards bringen nichts, wenn die Mitarbeiter sie nicht einhalten.“

Ina Schiering, IT-Expertin an der Ostfalia-Hochschule.

Risiko wird Firmen bewusster

Im November 2014 klagte G-Data-Vorstand Walter Schumann: Vielen mittelständischen Unternehmen fehle ein ganzheitlicher Ansatz für mehr IT-Sicherheit im Alltagsbetrieb. Auch das LKA-Niedersachsen mahnt zu mehr Aufmerksamkeit. Zwar schärfe sich bei den Firmen das Bewusstsein „für die dringende Notwendigkeit“ von IT-Sicherheitsmaßnahmen. „Gleichwohl müssen entsprechende Anstrengungen noch deutlich verstärkt werden.“

Jede Firma ohne Schutz gefährdet

Aus LKA-Sicht ist jeder Betrieb gefährdet, der Investitionen in IT-Sicherheitsmaßnahmen, die von Dienstleistern vorgenommen werden können, vernachlässigt. „Die Größe eines Unternehmens spielt eine untergeordnete Rolle, zumal bestimmte technische Maßnahmen zur Identifizierung von Schwachstellen automatisiert ablaufen.“ Deutlicher formuliert es Peter Peckedrath, Leiter der Innovationsberatungsstelle bei der IHK Braunschweig. Wer keine Firewall, keine aktuelle Virenschutzsoftware und Hardware mit Schutzvorrichtungen benutze, handele „grob fahrlässig“.

Nicht alle Firmen scheinen ausreichend geschützt. „Banken, Versicherungen, große Unternehmen, auch aus der produzierenden Industrie, sind vorbildlich“, meint Peckedrath. Nachholbedarf sehe er bei technologieorientierten Existenzgründern. Er befürchtet, dass ihnen das Geld fehlt, um sich den richtigen Schutz zuzulegen.

Heikler E-Mail-Verkehr

Ohne elektronische Post geht heute fast nichts mehr. Die Marktforscher von Radicati Group gehen davon aus, dass 2015 rund 204 Milliarden E-Mails weltweit täglich versendet werden. Gerade für Firmen ist das nicht ohne Risiken. SMAG-Chef Brandes sagt: „Alles, was geheim ist, versenden wir nicht per E-Mail.“ Zusätzlich arbeite das Unternehmen an Möglichkeiten der Verschlüsselung.

„Man sollte einen E-Mail-Provider wählen, der Perfect Forward Secrecy einsetzt“, rät Professor Ina Schiering, IT-Expertin an der Ostfalia-Hochschule. Dabei würden die Daten auf dem Weg zwischen den Mailservern verschlüsselt und seien später nur extrem schwer zu entschlüsseln. „Damit sind die größten Probleme auf dem Mail-Transportweg bereits beseitigt, wenn beide Mailserver das Verfahren Perfect Forward Secrecy bereitstellen“, sagt die IT-Expertin. Man könne E-Mails auch direkt verschlüsseln, etwa mit dem Programm Pretty Good Privacy. Allerdings brauche man technischen Sachverstand. „Auch hier müssen beide Kommunikationspartner das Verfahren einsetzen“, erklärt Schiering.

Firmennetzwerk abgrenzen

Das Firmennetzwerk gilt als Herzstück von Unternehmen. Die Inhalte, die dort lagern, können von der Mitarbeiter-Telefonliste über die komplette EDV bis hin zu streng geheimen Forschungsprojekten reichen. „Im internen Netzwerk ist es wichtig, verschiedene Sicherheitszonen einzurichten und den Zugriff auf Daten und Applikationen durch ein Rollen- und Rechtekonzept zu begrenzen“, erklärt Schiering. Vor allem auf sensible Daten dürfe nicht jeder Mitarbeiter Zugriff haben. „Für kleinere Unternehmen ist es oft schwer, das zu realisieren, wenn kein ausreichendes Know-how vorhanden ist“, sagt die Wissenschaftlerin.

Peckedrath warnt vor allem vor dem Zugriff auf Firmennetzwerke von außen – und zwar über ungesicherte WLAN-Zugänge. „Der gesamte Kommunikationsverkehr kann abgehört werden“, sagt der IHK-Experte. Durch einen offenen Zugang könnten Trojaner, Würmer oder andere Schad-Software ins Netzwerk gelangen. Damit könnte man die komplette EDV-Struktur eines Unternehmens lahmlegen oder zerstören.

Risiken beim Cloud Computing

Unter Cloud Computing versteht man die Ausführung von Programmen, die nicht auf dem eigenen Rechner liegen, oder das Speichern von Daten auf einem entfernten Rechenzentrum. Für Firmen hat das mehrere Vorteile. Sie können auf eigene Hardware und Speicher verzichten, sind weniger abhängig von eigenem IT-Personal und sparen damit Geld.

Doch ohne Risiken ist Cloud Computing nicht. „Wenn die Daten dort nur gespeichert werden sollen, kann man sie verschlüsselt ablegen“, rät Schiering. Sobald sie in Cloud Services verarbeitet würden, wie bei Google Docs oder der SAP Cloud, müssten sie dort unverschlüsselt vorliegen. „In dem Fall sollte man prüfen, ob die Sicherheitsstandards des Cloud Providers, nachgewiesen durch Zertifikate, die eigenen Sicherheitsanforderungen erfüllen“, sagt Schiering. Außerdem solle man die Rechtslage prüfen. „Viele der kostenfreien Cloud Dienste sichern sich in ihren AGBs und Datenschutzrichtlinien weitgehende Zugriffsrechte auf die dort gespeicherten Daten zu“, warnt die IT-Expertin von der Ostfalia.

Handy ausspioniert

Jeder weiß, wie praktisch ein Smartphone ist. So kann man auch von unterwegs auf E-Mails zugreifen oder Dateien lesen. Aber Vorsicht: Wenn mit Smartphones auf Firmendaten zugegriffen werden solle, sei es wichtig, dass das Gerät mit angemessenen Sicherheitsmechanismen ausgerüstet sei. Außerdem müsse es entsprechend der Sicherheits-Richtlinien des Unternehmens eingesetzt werden, sagt Schiering. „Gerade im privaten Bereich werden viele Apps installiert, die weitgehende Zugriffe auf das Gerät und den gesamten Speicher fordern“, warnt sie.

Die Abhöraffäre um Kanzlerin Angela Merkel hat es noch einmal deutlich gemacht. Technisch ist es machbar, Telefonate mitzuschneiden oder SMS mitzulesen. Dasselbe gilt für Internettelefonie. Wie das ARD-Politmagazin „Report“ kürzlich berichtete, werden bei der Internettelefonie Gespräche nicht verschlüsselt und können damit potenziell abgehört werden. Eine Verschlüsselung der Kommunikation muss durch zusätzliche Dienste erfolgen.

Das erschwert auch die Kommunikation für Firmen. Wer auf Nummer sicher gehen will, kann sich ein abhörsicheres Handy zulegen. Es kann die Gespräche vor der Übertragung verschlüsseln. Allerdings benötigt der Gesprächspartner ebenfalls ein solches Krypto-Handy. Alternativ können viele Handys durch eine entsprechende Software Gespräche verschlüsseln.

So schützen sich Firmen

„Mindeststandard ist es natürlich, Firewalls und Antivirenprogramme im eigenen Netzwerk einzusetzen“, sagt Schiering. Aber durch Trends wie Bring Your Own Device, Internet der Dinge und Smart Home sei das heute nicht mehr ausreichend. Schiering rät der Firmenleitung, zunächst herauszuarbeiten, was die Werte im Unternehmen sind und welche potenziellen Risiken existieren. Daraus könnten Sicherheitsanforderungen und Konzepte für die Umsetzung abgeleitet werden.

„Besonders wichtig ist es dabei, die Mitarbeiter mitzunehmen und ihnen die Sicherheitsziele transparent und verständlich zu machen“, sagt Schiering. Auch die höchsten Sicherheitsstandards brächten nichts, wenn die Mitarbeiter sie bewusst oder unbewusst nicht einhielten. Peckedrath sieht das ähnlich: „Verlässliche Mitarbeiter und eine Führungsspitze mit Sinn für das Wesentliche – Sind diese Voraussetzungen erfüllt, regelt sich der Rest von allein“, meint der IHK-Mann. Tatsächlich? Nun ja, nicht ganz. Eine absolute Sicherheit könne es nicht geben, wie die NSA-Affäre gezeigt hat, sagt Schiering.

Bis zu fünf Jahre Gefängnis

Egal, ob Spione die Telefonate abhören, E-Mails mitlesen oder Firmennetzwerke knacken – in jedem Fall handelt es sich um eine Straftat. Die Strafen fallen aber unterschiedlich hoch aus. „Für das Abfangen von Daten drohen bis zu zwei Jahre Gefängnis“, erklärt Jens Stanger, IT-Anwalt bei der Braunschweiger Kanzler Appelhagen. Unter dem Abfangen verstehe man beispielsweise das Mitlesen von E-Mails. Bis zu drei Jahre Gefängnis oder eine Geldstrafe drohen, wenn man Daten ausspäht. Darunter falle beispielsweise das Eindringen in Firmennetzwerke, sagt Stanger. Noch härter kann es Kriminelle treffen, wenn sie Telefonate abhören und damit das Telekomgeheimnis verletzen. In diesem Fall könne es bis zu fünf Jahre Gefängnis geben, weiß der IT-Anwalt.

In der nächsten Folge lesen Sie

Die Digitalisierung ist längst nicht abgeschlossen. Aber wohin wird die Entwicklung führen? Professor Sándor Fekete von der TU Braunschweig blickt in die Zukunft.

WÖRTERBUCH DER DIGITALISIERUNG

Hacker: Menschen, die darauf spezialisiert sind, unerkannt in fremde Computer einzudringen, werden Hacker genannt. Ihre Arbeit ist oft verboten, kann aber auch nützlich sein: Zum Beispiel, wenn Hacker für IT-Firmen Sicherheitslücken in Computern entdecken.

Virus: Der Ursprung des Begriffs liegt nahe – ein Computer, der von einem Virus befallen ist, ist krank. Oft handelt es sich bei Viren um Dateien, die ohne das Wissen des Besitzers auf dem Rechner platziert werden.

Firewall: Um den Computer vor illegalen Zugriffen zu schützen, verwenden viele Rechner eine Firewall. Diese funktioniert wie eine echte Mauer: Sie soll verhindern, dass schädliche Dateien auf den Rechner gelangen.

Trojaner: Fast wie das legendäre trojanische Pferd ist auch der digitale Trojaner aufgebaut. Für den Besitzer unerkannt wird eine Datei auf einem Computer platziert, die diesen dann von innen angreift. *kop*