In fremder Hand

Wie ein Betrieb aus Simmerath zum Opfer von Hackern wurde – und welche Ratschläge vier IT-Experten aus unserer Region zur Vermeidung von Cyber-Angriffen geben

VON DANIEL BOSS

Diesen Tag im Herbst des vergangenen Jahres wird Heinz Thoma nicht so schnell vergessen. Es war nur eine kleine Unachtsamkeit – und am Ende ein großes Unglück. Eines, das seine Beratungsfirma aus Simmerath, die imatec GmbH, in einen Ausnahmezustand versetzte. „Ich habe mehr als nur eine schlaflose Nacht verbracht", erzählt der Geschäftsführende Gesellschafter im Rückblick. Es begann vermeintlich harmlos. Im E-Mail-Eingang des Unternehmens landete eine „Bewerbung". Keine große Überraschung, hatte „imatec" doch kürzlich eine Stellenanzeige geschaltet. „Der Eindringling war geschickt getarnt", erzählt Thoma: „Die E-Mail sah völlig unverdächtig aus, es gab einen normal wirkenden Absender." Nur eine Kleinigkeit stimmte nicht: Der mitgeschickte Anhang hatte die Datei-Endung „pdf.pdf". Doch die Mitarbeiterin am Computer maß dieser Dopplung keine große Bedeutung zu. Ein kurzer Klick aufs Dokument – und schon nahm das Unheil seinen Lauf...

Datenklau mit Dunkelziffer: Laut einer „Norton by Symantec"-Studie sind 38 Prozent der Internetnutzer in Deutschland Opfer von Cyber-Kriminalität mit einem bundesweiten Schaden von 2,2 Milliarden Euro geworden – wobei die Polizei-Statistik nur wenige Fälle registriert, die zur Anzeige gebracht werden.

Denn die Mitarbeiterin hatte einem „Erpresser-Virus" die Tür zum Betrieb geöffnet. Hinter der – natürlich falschen – Absender-Adresse verbargen sich unbekannte Cyber-Kriminelle auf der Suche nach dem schnellen Geld. „Das Virus begann sofort damit, unsere Daten zu befallen", sagt Thoma. Als das Team realisierte, was passiert war, nahmen die Mitarbeiter den betroffenen Rechner schnell aus dem Netzwerk. Aber zu spät. „Unser Server war bereits infiziert." Sämtliche Office-Dateien waren nicht mehr nutzbar. „Von diesen Dokumenten leben wir zu 80 Prozent, das war fatal für uns", schildert der Geschäftsführer das Ausmaß der Attacke.

Digitales Lösegeld

Doch damit nicht genug: Es dauerte nicht lange, da erreichte eine weitere E-Mail das in helle Aufregung versetzte Büro. Tenor: Wenn man das Virus wieder loswerden wolle, müsse man so-und-so-viele Bitcoins auf ein bestimmtes Konto transferieren. In Krypto-Währung umgerechnet, wären es laut Thoma „einige zehntausend Euro" Lösegeld gewesen. Er habe einen kurzen Moment darüber nachgedacht, der Erpressung nachzugeben, gesteht der Unternehmer. „Wir konnten zu diesem Zeitpunkt überhaupt nicht abschätzen, wie hoch der Schaden war und noch werden könnte." Offensichtlich war nur, dass nichts mehr lief. Niemand habe mehr arbeiten können.

Unter anderen Umständen hätte diese perfide E-Mail für „imatec" schnell existenzbedrohend werden können. Doch die Simmerather hatten das begehrte Glück im Unglück. „Wir verfügten über eine sehr gute Datensicherung, nämlich über einen eigenen Back-up-Server und Festplatten, die mobil und außerhalb des Büros gelagert werden", erläutert Thoma. Mit Hilfe eines externen IT-Experten habe man das befallene System „plattgemacht" und es dann „in aller Vorsicht" wieder hochgefahren. Alles Wesentliche konnte gerettet werden. Doch zwei Arbeitstage waren weg, der Schaden bereits immens. Thoma erstattete Anzeige, versprach sich aber nichts davon. „Diese Leute erwischt man nicht. Deren Server stehen ja nicht in Aachen oder Köln, sondern irgendwo in der Welt." Inzwischen sei das Verfahren eingestellt worden.

Das hat Konsequenzen

Heinz Thoma und die imatec GmbH haben mehrere Konsequenzen aus dem Cyber-Angriff gezogen: „Beim leisesten Verdacht werden E-Mails nicht mehr direkt geöffnet, sondern zunächst auf einen eigenen abgekoppelten Server gelegt", sagt der Unternehmensleiter. Außerdem gelte für fremde USB-Sticks und DVDs ein striktes Hausverbot. Ferner berät das Unternehmen, das bis dato unter anderem auf Qualitätsmanagement und Arbeitsschutz spezialisiert war, nun auch in Sachen IT-Forensik. „Wir haben am eigenen Leib schmerzhaft erfahren, was heute passieren kann, und wir wollen verhindern, dass andere Betriebe den gleichen oder einen ähnlichen Fehler machen", sagt Diplom-Ingenieur Thoma. Man benötige heutzutage ein „Informationsschutz-Management-System" (ISMS). Mit der Zertifizierung dieses Systems nach „ISO 27.001" will sich der Geschäftsführer nun auch den „Segen" einer externen Stelle einholen.

Pentests: Eingekaufte Überfälle

Erpressungs-Trojaner vom Typ des Simmerather Falls seien gang und gäbe, sagt Jens Liebchen. Betroffene dürften noch froh sein, wenn sich die Erpresser melden. „Dann wissen sie wenigstens, dass sie ein Problem haben, denn das Virus kann ja auch Tage oder Wochen im System schlummern", sagt der Geschäftsführer der in Aachen ansässigen RedTeam Pentesting GmbH. Auf diese Weise könnten vollkommen unbemerkt Informationen abgeschöpft oder Daten manipuliert werden – mit katastrophalen wirtschaftlichen Folgen. Das von Liebchen und seinem Kollegen Patrick Hof geführte Unternehmen bietet individuelle Penetrationstests – kurz: „Pentests" – an, die von einem Team spezialisierter IT-Sicherheitsexperten vorgenommen werden. Dadurch würden Sicherheitslücken in Netzwerken, Anwendungen oder Geräten aufgedeckt und könnten anschließend behoben werden.

Der Betrieb, der heute mit zehn Mitarbeitern weltweit und branchenübergreifend aktiv ist, hat seinen Ursprung in einer Forschungsgruppe der RWTH Aachen. „Ein Penetrationstest ist ein Angriff – zwar im Auftrag eines Unternehmens, aber es bleibt ein Angriff", erklärt Liebchen. Wie bei allen Attacken, könne dabei auch etwas schiefgehen, obgleich das Risiko überschaubar sei. „Aber als Student konnten und wollten wir dieses Wagnis nicht

Foto: © Amir Kaljikovic – Fotolia.com

Einmal einbrechen, bitte: Wer sein IT-System auf Sicherheitslücken untersuchen lassen möchte, kann dazu Unternehmen wie das Aachener „RedTeam Pentesting" beauftragen.

tragen", sagt er. Die Gündung einer GmbH war die Folge. Das „RedTeam" betracht sich nicht als klassischen IT-Dienstleister, sondern bietet ausschließlich Pentests an. „Wir lassen die Attacken für sich sprechen. Nichts ist so überzeugend, um größere Sicherheits-Investitionen zu tätigen, als die Erfahrung am eigenen Leib", sagt Liebchen. Pentests seien auch für kleine Betriebe interessant; allerdings komme es auf die Kosten-Nutzen-Rechnung an. Klar ist für ihn: „Wer IT-Sicherheit nicht ernst nimmt, ist früher oder später weg vom Markt. Größere Pannen kann sich vielleicht Facebook einmal erlauben – ein Start-up-Betrieb aber keinesfalls." Oft könnten sogar Leib und Leben von Sicherheitslücken abhängig sein, zum Beispiel in Krankenhäusern: „Moderne OP-Säle sind komplett vernetzt", betont Liebchen.

Mit einem gewissen IT-Risiko müsse der Mensch des 21. Jahrhunderts leben: „Hundertprozentige Sicherheit gibt es nicht. Wer damit wirbt, der lügt", sagt der Unternehmer. Wäre dieser Rundum-Schutz mit Garantie möglich, hätten die großen Software-Produzenten „längst entsprechende Lösungen präsentiert, mit denen sich logischerweise viele Milliarden Euro verdienen ließen". Selbstberuhigung nach dem Motto „Unser Betrieb ist für Hacker doch gar nicht interessant" lässt Liebchen nicht gelten. Man könne schließlich auch Zufallsopfer werden. Und das ebenso im privaten Bereich: „Jeder moderne Fernseher ist heute ein Rechner mit Internetzugang. Man kann sich nicht mehr abschotten."

Das Auto als rollender Computer

Auch im Automobilbereich geht es längst nicht mehr nur um Air-bags und Knautschzonen. „Moderne Autos sind rollende Computer mit einer überbordenden Komplexität und gut 100 Millionen Zeilen Programmier-Code", sagt Thomas Käfer, der sich beruflich seit vielen Jahren mit diesem Thema befasst. Ein F22-Kampfjet habe gerade einmal zwei Millionen und Windows 7 etwa 38 Millionen Zeilen. „Mit dem Ziel, diese Fahrzeuge immer mehr untereinander und mit Verkehrsinfrastrukturen zu vernetzen und sie schließlich voll-automatisiert oder gar autonom fahren zu lassen, haben sich die Hersteller einiges vorgenommen", meint Käfer: „Betrachtet man aber, wie unbedarft und fahrlässig aktuelle Systeme in Fahrzeugen entwickelt und realisiert werden, dann ist das Vertrauen in die Sicherheit unbegründet", kritisiert der Diplom-Ingenieur aus Würselen. Er ist mit seinem IT-Systemhaus seit 1990 selbstständig tätig und beschäftigt sich regelmäßig mit Fragestellungen der IT-Sicherheit – und mit der forensischen Auswertung von modernen Fahrzeugen und IT-Systemen, die mit diesen gekoppelt sind.

„Wir haben am eigenen Leib erfahren, was passieren kann. Wir wollen verhindern, dass andere Unternehmen den gleichen oder ähnliche Fehler machen."

Heinz Thoma, Geschäftsführender Gesellschafter der imatec GmbH

„Davon sind wir weiter entfernt, als so manch einer wahrhaben will"

Die Erwartungshaltung des allgemeinen Autokäufers liege – „begünstigt durch vielfach oberflächliche und unkritische Berichterstattung in den Medien, durch vollmundige Werbeversprechen sowie Strategieankündigungen der Automobilhersteller" – deutlich über dem, was in Bezug auf Qualität und Funktionsumfang an Fahrerassistenzsystemen und Vernetzung in aktuellen Modellen tatsächlich angeboten werde. „Von dem mittelfristig angepeilten Ziel sowohl der Hersteller als auch der Politik und der Verkehrsexperten, in wenigen Jahren zumindest in bestimmten Arealen Autos selbstständig fahren zu lassen, sind wir weiter entfernt als so manch einer zugeben oder wahrhaben will."

IT-Sicherheit im Auto erst im Nachhinein „angehängt"

Und dabei gehe es nur um den „Safety"-Aspekt, also die funktionale Sicherheit. Bei der IT-Sicherheit sehe es unterdessen noch schlechter aus. „Immer wieder gelingt es den ‚guten Hackern', in die in Autos verbauten beziehungsweise damit gekoppelten IT-Systeme einzudringen, die Kontrolle über Funktionen oder das gesamte Fahrzeug zu übernehmen oder personenbezogene Daten auszulesen." Und die „guten" – also die nichtkriminellen – Hacker redeten darüber. „Anzunehmen ist daher, dass sie nur die berühmte Spitze des Eisbergs ausmachen." Die Automobilindustrie beginne gerade erst damit, sich auch über IT-Sicherheit im Fahrzeug Gedanken zu machen. Teilweise werde versucht, Security ins fertige Produkt „hineinzutesten" oder „anzuhängen" – für Käfer ein untaugliches Konzept, denn „IT-Sicherheit und Datenschutz gehören bei jedem Produkt in den Kern der Entwicklung".

INFO

„MStorm": Aachener IT-Betriebe arbeiten an einer neuen Lösung gegen Phishing und Malware

Die beiden Aachener Unternehmen „X41 D-SEC GmbH" und „Abovo-IT UG (haftungsbeschränkt)" haben eigenen Angaben zufolge mit führenden Branchenexperten die Software „MStorm" entwickelt. Sie soll die Zahl der Fälle minimieren, in denen Mitarbeiter auf E-Mails mit Schadprogrammen oder Phishing-Angriffen hereinfallen. Die neue Software verschickt Phishing- und Malware-E-Mails und misst, welche Arten dieser Nachrichten durch die Filter des Unternehmens in die Postfächer der Mitarbeiter gelangen können. Danach soll das Programm erfassen, welche Mitarbeiter auf Phishing und Malware falsch reagieren, um sie anschließend mit einer Online-Schulung samt Quiz für den richtigen Umgang mit schädlicher „Post" zu sensibilisieren. Der Kern von „MStorm" sei in einem Forschungsprojekt für einen US-Konzern zum Benchmarking von E-Mail-Filtern entwickelt worden. Im Oktober starte das erste Projekt bei einer deutschen Versicherungsgesellschaft.

Auf Bremsen und Lenkung schauen Kfz-Experten im Rahmen vorgeschriebener, regelmäßiger Prüfungen. „Wenn man sieht, wie oft heutige Betriebssysteme im Office-Bereich aktualisiert werden müssen, dann erkennt man, dass ein Update der Software bei einer jährlichen Inspektion eines Fahrzeugs ein viel zu langer Zeitraum ist. Wenn sie dabei denn überhaupt aktualisiert wird", sagt Käfer. Ein Prüfzyklus erstmals nach drei Jahren – wie etwa beim TÜV – sei ebenfalls zu lang, wobei derzeit auch hier noch nichts im Bereich der IT-Sicherheit kontrolliert werde: „Der Fahrer würde die Software seines Autos gern aktualisieren lassen, kann es oft aber gar nicht, da es weder Strategien noch Mechanismen für regelmäßige Updates im Automotive-Bereich gibt."

„Wer IT-Sicherheit nicht ernst nimmt, ist früher oder später weg vom Markt. Größere Pannen kann sich vielleicht Facebook einmal erlauben – ein Start-up-Betrieb aber keinesfalls."

Jens Liebchen,
Geschäftsführer der RedTeam Pentesting GmbH

Angriff durch die Hintertür

In Sachen IT-Sicherheit sieht Ralf Koenzen, Geschäftsführer der LANCOM Systems GmbH, grundsätzlich zwei große Risiken: „Versteckte Zugriffsmöglichkeiten in der Hardware – sogenannte Backdoors – und schwerwiegende Schwachstellen in der Software, die nicht geschlossen werden." Das Unternehmen mit gut 330 Mitarbeitern, von denen die meisten am Hauptsitz in Würselen tätig sind, bietet Netzwerklösungen für Geschäftskunden und die öffentliche Hand an. „Beim Router, über den meistens der Datenverkehr eines Unternehmens läuft, bildet der unerwünschte Zugriff über eine Hintertür ein erhebliches Sicherheitsrisiko", erklärt Koenzen. Schließlich könnten Dritte auf diese Weise sensible Daten auslesen und manipulieren oder direkt auf das Netz zugreifen. Das Phänomen „KRACK" sei indes ein prominentes Beispiel für Sicherheitslücken in der Software, deren Erkennung noch lange nicht zwangsläufig die Gefahr bannt: „Nachdem die Schwachstelle entdeckt wurde, haben vor allem die renommierten Hersteller Updates geliefert und die Lücke geschlossen", erklärt Koenzen, „aber viele Geräte – vor allem Handys und ‚Smart Devices' – haben aus Kostengründen oder wegen technischer Limitierung gar kein Update erhalten. Das Ergebnis: Bei Millionen von Geräten klafft die Lücke immer noch – ein willkommenes Einfallstor für Cyber-Kriminelle."

„Betrachtet man, wie unbedarft und fahrlässig aktuelle Systeme entwickelt und realisiert werden, die im Auto verbaut sind oder damit gekoppelt werden, dann ist das Vertrauen in die Sicherheit unbegründet."

Thomas Käfer,
Geschäftsführer „Käfer IT Systeme e.K."

„Sicherheit ist manchen Herstellern zu teuer"

Der IT-Unternehmer appelliert an staatliche Behörden und an die Politik: „Was wir in Deutschland und Europa zwingend brauchen, sind höhere Markteintrittsbarrieren für unsichere IT-Produkte!" Es müsse verhindert werden, dass Hardware und Software, die nur wenig bis gar keinen Wert auf Sicherheit lege, unsere Märkte überfluten. „Sicherheit wird von einigen Herstellern vernachlässigt, weil sie eben teuer ist – und weil keine verpflichtenden Vorgaben existieren." Eine gesetzliche Update-Pflicht und feste IT-Sicherheits-Mindeststandards, die für alle internetfähigen Geräte gelten, würden Koenzen zufolge Abhilfe schaffen. Darüber hinaus müsse mehr Transparenz geschaffen werden. „Verbraucher und Betriebe stehen vor der schwierigen Aufgabe, sichere von unsicheren Lösungen zu unterscheiden. Hilfreich wären dabei Basiszertifizierungen von IT-Produkten oder freiwillige marktaugliche IT-Sicherheitszertifizierungen für Unternehmenslösungen."

Auch Koenzen betont indes: „Absolute Sicherheit in der IT gibt es nicht." Die Vergangenheit habe gezeigt, dass Sicherheitslücken oft viele Jahre lang in Betriebssystemen mehr oder weniger unentdeckt existieren könnten. Selbst hochsichere Systeme wiesen keinen hundertprozentigen Schutz auf. Der Unternehmer rät deshalb zu einer sorgfältigen Überwachung von Risiken und zu einer ebenso genauen Planung und Umsetzung von Sicherheitsmaßnahmen. Heinz Thoma aus Simmerath muss er davon jedenfalls nicht mehr überzeugen... ■

NACHGEFRAGT

Foto: LANCOM Systems GmbH

Ralf Koenzen,
Geschäftsführer der LANCOM Systems GmbH

„Bewusstsein schaffen und Anbieter prüfen"

WN: Was sollten Unternehmen von sich aus tun, um in punkto IT-Sicherheit möglichst gut aufgestellt zu sein?

Koenzen: Wichtig ist, dass bei den Mitarbeitern ein Bewusstsein, ein Verständnis für IT-Sicherheit geschaffen wird. Dazu gehört ganz grundlegendes Wissen – zum Beispiel, dass ich nicht einfach E-Mail-Anhänge von unbekannten Absendern öffne. Diejenigen Abteilungen, die mit der Beschaffung von IT-Lösungen betraut sind, sollten sich die Hersteller und Anbieter der benötigten Hardware oder Software genau anschauen: Welchem nationalen Recht unterliegt der Anbieter? Wie werden bei Cloud-Diensten meine sensiblen Daten verarbeitet? Kann der Router-Hersteller eine Backdoor-Freiheits-Erklärung vorweisen? Unternehmen klären am besten auch im Voraus, ob und wie lange ein Hersteller Sicherheits-Updates zur Verfügung stellt.