INTERVIEW

Dr. Tilman Frosch, Geschäftsführer von G DATA I Advanced Analytics, im Gespräch

“Wir schaffen bezahlbare IT-Sicherheit auch für KMU – das Rückgrat der deutschen Wirtschaft“

Medien berichten zunehmend über das Thema IT-Sicherheit. Aus Ihrer Erfahrung: Wie verändert sich die Bedrohungslage für Unternehmen? Und wie hoch sind die Schadenssummen?

Dr. Frosch: Unternehmen werden mittlerweile sehr gezielt von Kriminellen angegriffen. Das Spektrum ist dabei breit: Manchmal ist ein Unternehmen schlicht Beifang, aber manche Attacken sind gut vorbereitet und die Strategie an die jeweilige Firma angepasst. Schadsoftware ist dabei das am häufigsten eingesetzte Werkzeug der Angreifer, aber man darf auch das Problem von Innentätern nicht klein reden. Nach Angaben des Branchenverbandes BITKOM waren in den vergangenen zwei Jahren drei von vier Unternehmen von Sicherheitsvorfällen betroffen.

Wir sehen aber nicht nur eine Zunahme der Angriffe, sondern auch neue Strategien. So passen die Kriminellen die Schadenssummen von Erpressertrojanern so an, dass das Unternehmen sich die Zahlung der Summe gerade noch so leisten kann. Das ist ein Vorgehen, das wir so bislang nur aus größeren Unternehmen kannten. Kleine und mittelständische Unternehmen bekamen bis letztes Jahr Standardpreise, egal ob nun ein Privatrechner oder ein ganzes Unternehmensnetzwerk kompromittiert war. Das ändert sich gerade.

„Die Schadenssummen sind so vielfältig, wie die Unternehmen selbst“

Die Schadenssummen sind so vielfältig, wie die Unternehmen selbst. Für einige Unternehmen ist schon ein Schaden von mehreren tausend Euro kaum zu verkraften. Wir kennen jedoch auch Lösegeldforderungen von mehreren hunderttausend Euro. Hinzu kommt das Risiko, Opfer der massiven Kollateralschäden zu werden, verursacht etwa durch Verschlüsselungstrojaner wie WannaCry und NotPetya. Das kann den Containerriesen Maersk genauso treffen wie die Bäckerei um die Ecke.

Die Kriminellen werden außerdem immer schneller. Wir haben im vergangenen Jahr beobachtet, dass die Täter bis zu 200 neue Versionen von bestimmten Malware-Familien pro Tag an die Opfer bringen. Gleiche Schadsoftware, neue Verpackung. Das bedeutet: Manchmal kommt alle sieben Minuten eine neue Version des Schadprogrammes in Umlauf.

Datensicherheit für kleine Unternehmen:
www.lexware.de/gdata

Um Cyberkriminellen einen Schritt voraus zu sein, bedarf es daher neuer Technologien. Wir bei G DATA investieren deshalb seit 2008 massiv in proaktive Komponenten. Zuletzt in DeepRay, eine Technologie mit der uns die häufig wechselnde Umverpackung von Malware nicht mehr interessieren muss.

Darüber hinaus: Schadsoftware ist zahlenmäßig das häufigste Tatwerkzeug, aber nicht das einzige. Deshalb ist G DATA auch kein reiner Anbieter von Antivirenlösungen mehr. Unter dem Begriff Cyber Defense Services verstehen wir einen ganzheitlichen Schutz unserer Kunden gegen Cybercrime. Wir bieten von der Endpoint-Protection über Security Assessments bis hin zu einem eventuell notwendigen Notfalleinsatz (Stichwort: Incident Response) schon viele notwendige Dienste aus einer Hand an – ein Bereich unseres Portfolios, der einer stetigen Entwicklung unterliegt und dessen Relevanz steigt.

Aus Ihrer Erfahrung: Was sind typische Schwachstellen in der IT von KMU?

Dr. Frosch: Wir sehen gerade bei kleinen und mittleren Unternehmen immer wieder, dass Unternehmensnetze sehr organisch gewachsen sind. Dabei wächst dann zwar die Komplexität; die Sicherheit wächst dabei aber meist nicht mit. Das beginnt damit, dass die Netzwerke sehr flach aufgebaut sind, das heißt, unterschiedliche Bereiche des Unternehmens befinden sich in ein und demselben Netzwerk – ohne eine sinnvolle Abgrenzung der Bereiche. Das erschwert die Eingrenzung von Sicherheitsvorfällen ganz erheblich.

Zudem lassen sich alle Betriebssysteme heute recht ordentlich härten – also so konfigurieren, dass es ein Angreifer möglichst schwer hat, bevor die ebenfalls notwendigen Schutzmechanismen wie Endpoint-Security greifen. Diese Möglichkeiten werden selten genutzt, da sie eine tiefgehende Beschäftigung mit dem Thema erfordern. IT ist personell aber meist ohne großen Spielraum ausgelegt, denn IT ist nicht unbedingt günstig.

Ab einer gewissen Größenordnung ist es sinnvoll, einen fachkundigen Mitarbeiter mit dem Thema IT-Sicherheit zu betrauen. Aber für die Mehrheit der Unternehmen, und wir sprechen hier von mehr als 99 Prozent der Unternehmen in der EU, ist das nicht wirtschaftlich. Ein guter Security Consultant dagegen kann hier als externer Berater einen großen Unterschied für die Verteidigungsfähigkeit des Unternehmens machen.

Oftmals wird die IT auch komplett durch Dienstleister gemanagt. Hier heißt es „Augen auf“ bei der Auswahl. Im Zweifel kann auch hier externe Kompetenz hilfreich sein, wenn es um die Vertragsgestaltung mit dem verwaltenden Systemhaus geht.

Denn wir sehen leider immer wieder IT-Dienstleister, die selbst nicht über die notwendigen Sicherheitsprozesse verfügen. Solche Fehler schlagen dann schnell auf die Netzwerke der Kunden durch und machen diese angreifbar.

Können Kleinunternehmen und Mittelständler sich IT-Sicherheit angesichts der Bedrohungslage überhaupt leisten?

Dr. Frosch: Die Frage muss doch anders herum gestellt werden: Können Sie es sich leisten, NICHT in IT-Sicherheit zu investieren? Wir merken seit Jahren, dass die Bereitschaft wächst, in Sicherheit zu investieren – nicht erst seit der DSGVO. Das Problem sehe ich für viele Unternehmen eher auf der Angebotsseite.

Denn die meisten Lösungen jenseits von Endpoint-Protection und Security Gateways – also Antivirenprogramme und Firewalls – richten sich von ihrer Konzeption und vom Preis her an Enterprise-Kunden mit vielen tausend oder sogar hunderttausend Arbeitsplätzen. Das kann ein Mittelständler oder Kleinunternehmer sich natürlich nicht leisten. Wir schaffen bezahlbare IT-Sicherheit auch für Kleinunternehmen und den Mittelstand. Zu tun gibt es allemal genug, der Bedarf ist vorhanden.

Ein besonderes Problem für Kleinunternehmen ist, dass sie IT-Sicherheit bislang häufig nicht in ihre Budgetplanung einbringen. Wer hier investiert, dem fehlt am Ende unter Umständen die nötige Marge zum Überleben. Denn es wird immer Konkurrenten geben die bereit sind, das Risiko ungeschützter IT-Systeme einzugehen.

„Ein besonderes Problem für Kleinunternehmen ist, dass sie IT-Sicherheit bislang häufig nicht in ihre Budgetplanung einbringen.“

Nur etwa 0,2 Prozent der Unternehmen in der EU sind im eben beschrieben Enterprise-Umfeld zu finden. Alle anderen – von der kleinen Bäckerei mit wenigen Angestellten bis zum regionalen Architekturbüro oder Bauunternehmen mit 50 Mitarbeitern – haben bisher nur bedingt Zugang zu dem, was wir als Stand der Technik betrachten. Das wollen wir bei G DATA mit unseren Angeboten ändern.

Welche Angebote meinen Sie?

Dr. Frosch: Gerade kleinere Unternehmen sollten das Thema IT-Sicherheit ganzheitlich betrachten. Der erste sinnvolle Schritt ist oft ein Security Assessment – also eine Erhebung des Ist-Zustands der IT und der IT-Prozesse aus der Sicherheitsperspektive. Wir klopfen mit unseren Kunden eine lange Liste von potenziellen Problemstellen ab und nehmen uns dann mit einem Schwachstellenscan von außen und auch von innen die tatsächlich vorhandene Infrastruktur vor. Schon das Assessment liefert meist ein deutliches Bild; und ein Schwachstellenscan ist eine kostengünstige Möglichkeit, einen ersten Eindruck der Realität im Unternehmensnetz zu bekommen. Zwischen glauben was man hat und wissen was man hat, existieren oft gewaltige Unterschiede – Stichwort Schatten-IT.

Wir sehen in unserer Arbeit allerdings fast täglich, dass geschickt verbreitete Malware in Kombination mit Schwachstellen im Sicherheitsmanagement für enormen Schaden sorgen kann. Dabei kann selbst etwas eigentlich sehr Einfaches, wie ein Erpressungstrojaner, ein Unternehmen in den Konkurs treiben, wenn alle Daten verschlüsselt und zuvor die Backups gelöscht wurden.

„Unternehmen sollten ihre eigene Bedrohungslage klären“

Bevor ich mich aber als Unternehmen entscheide, in bestimmte Technologien oder Prozesse zu investieren, sollte klar sein, was gegen wen zu schützen ist. Ein Threat Modelling mit professioneller Unterstützung hilft, Investitionen in IT-Sicherheit sinnvoll zu steuern. Dabei wird systematisch geklärt, vor welchen Risiken die Firma sich schützen kann und sollte und was genau eigentlich geschützt werden muss. Die öffentliche Diskussion fokussiert sich häufig auf technisch extrem hochentwickelte Angriffe mit bislang unbekannten Schwachstellen – Zero-Day-Exploits genannt. Das ist aber gerade für kleinere Unternehmen gar nicht relevant. Anders ausgedrückt: Geheimdienste egal welchen Landes sind nur für wenige Unternehmen die relevanteste Gefahr.

Ist ein Penetrationstest ein guter erster Schritt in Richtung sichere IT?

Dr. Frosch: Erstmal: Was bedeutet sichere IT? Unser Ziel ist immer ein verteidigungsfähiges Unternehmen. Sicherheitsvorfälle passieren. Den Unterschied macht, wie ein Unternehmen damit umgehen kann. Ein umfassender Penetrationstest, also die intensive Analyse eines Unternehmens auf mögliche Schwachstellen in der IT, ist extrem wertvoll und kann einen guten Überblick über die Angriffsoberfläche eines Unternehmens liefern. Aber er erfordert organisatorische Reife, um auf die Ergebnisse zu reagieren. Gerade kleinere Unternehmen haben im ersten Schritt von einem Security Assessment mehr umsetzbare Ergebnisse für weniger Aufwand. Ganz klar übrigens ein Thema, das wir in Zukunft mehr in Fläche bringen werden, genau weil es für wirklich jeden unserer Kunden konkrete, zielführende Ergebnisse liefert.

Immer wieder heißt es: Mitarbeiter sind das schwächste Glied der Kette. Wie mache ich Mitarbeiter stattdessen zur ersten Abwehrlinie?

Dr. Frosch: Die wichtigste Ressource eines Unternehmens sind seine Mitarbeiter, auch in Bezug auf ein ganzheitliches IT-Sicherheitsmanagement. Phishing und Social Engineering gehören noch immer zu den wirkungsvollsten Taktiken, um Unternehmensnetzwerke zu kompromittieren. Aufmerksamkeits-Trainings (engl. Awareness-Trainings), die Mitarbeiter an der richtigen Stelle abholen und aktiv für das Thema motivieren sind ein wichtiger Bestandteil einer jeden IT-Sicherheitsstrategie, ob persönlich vor Ort oder als Computer-basierte Trainings. Nicht zuletzt ist Awareness auch ein Compliance-Thema für IT-Verantwortliche und Geschäftsführung.

Präsenztrainings sind auch hervorragend zur Vertiefung bei bestimmten Zielgruppen geeignet. So könnte die Personalabteilung im sicheren und datenschutzkonformen Umgang mit Bewerbungsunterlagen geschult werden und andere Unternehmensbereiche im sicheren Umgang mit sozialen Medien und dem mobilen Arbeiten.

Weitere Informationen zum Angebot von G Data können Sie hier anfordern: www.lexware.de/gdata