Eine fünfstündige Anhörung im US-Kongress: Datensicherheit ist mittlerweile eine Angelegenheit von globaler Tragweite, wie der Fall Facebook zeigt.

Foto: Blind

~ CYBERSECURITY ~

Krieg der Daten 4.0

Die Digitalisierung von Wirtschaft und Gesellschaft lässt Cybersecurity zu einem Megatrend avancieren.

Autor: Prof. Norbert Pohlmann, Gelsenkirchen

Informationstechnik (IT) und das Internet sind Motor und Basis für das Wohlergehen unserer modernen und globalen Informations- und Wissensgesellschaft. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen unserer IT-Systeme, wie Endgeräte, Server und Netzkomponenten nicht sicher genug konzipiert und aufgebaut sind, um den Fähigkeiten von intelligenten Hackern standzuhalten. Täglich können wir den Medien entnehmen, wie sich kriminelle Hacker die unzureichende Qualität der Software für erfolgreiche Angriffe zu Nutze machen, Malware installieren, Passwörter sowie Identitäten stehlen, mit Fake News Wahlen beeinflussen sowie unsere Endgeräte ausspionieren. Wenn wir diese Probleme in der Zukunft nicht mit wirkungsvolleren Cybersicherheitslösungen in den Griff bekommen und damit Vertrauen aufbauen, wird uns eine nachhaltige Digitalisierung nicht gelingen.

Der Schaden im Bereich Wirtschaftspionage in Deutschland beläuft sich laut einer Bitkom Studie auf 55 Milliarden Euro im Jahr. Ein derartig hohe Schadenssumme können sich Staaten wie Deutschland nicht leisten, insbesondere, weil er kontinuierlich größer wird. Die Angreifbarkeit der IT und des Internets nimmt zu und Werte, die als Bits und Bytes auf unseren IT-Systemen zur Verfügung stehen, werden immer risikobehafteter für die einzelnen Unternehmen, die Bürger und den Staat.

Eine weitere und immer bedeutsamere Herausforderung ist der Cyberkrieg. Angriffe auf Kritische Infrastrukturen, wie Energie-, Wasser-, Lebensmittel-, Gesundheitsversorgung, stellen eine prinzipiell höhere Angreifbarkeit unserer Gesellschaft dar, sie bilden eine neue Ebene der existenziellen Bedrohung und werden daher die ökonomische Relevanz der Cybersicherheitsindustrie stark vergrößern.

Dank Stuxnet haben wir lernen müssen, dass mit einem verhältnismäßig geringen Kostenaufwand von rund neun Millionen US-Dollar für eine intelligente Malware politische Ziele einfach und sehr erfolgreich umsetzbar sind. Mit der intelligenten Malware Stuxnet konnten US-Amerikaner und Israelis die Uranaufbereitung im Iran um zwei Jahre verzögern können.

Die schreckliche Alternative wäre gewesen, hunderttausend Soldaten in den Iran zu entsenden. Das hätte nicht nur Kosten von mehreren Milliarden US-Dollar verursacht, sondern auch unzählige Menschenleben aufs Spiel gesetzt. Wir müssen uns auf diese neue Wirklichkeit von Cyberkrieg professionell einstellen und deutlich mehr und wirkungsvollere Cybersicherheitslösungen einsetzen, um uns als Gesellschaft zu schützen.

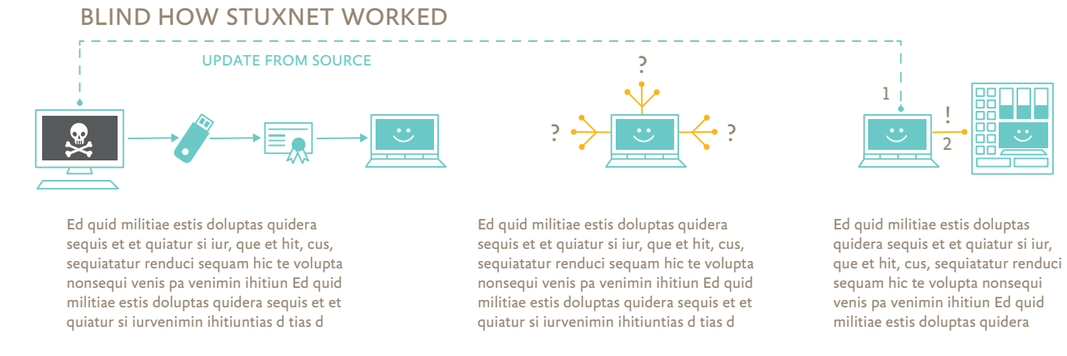
Wir haben uns im Rahmen mehrerer Befragungen über Schäden und Cybersicherheitstechnologien bei Unternehmen auch mit der Frage auseinandergesetzt, wie hoch die Ausgaben für Cybersicherheit in Unternehmen sind. Die Ergebnisse der Befragungen zeigen auf, dass die Unternehmen im Schnitt 0,1% ihres Gesamtumsatzes in Cybersicherheitslösungen investieren - ohne Dienstleistungen. Bei einem Bruttoinlandsprodukt von 3,7 Billionen US-Dollar wären das 3,7 Milliarden für 2017 allein in Deutschland. Das weltweite Bruttoinlandsprodukt lag 2017 bei 79,3 Billionen US-Dollar. Danach wären dies 79,7 Milliarden Dollar Ausgaben für Cybersicherheitsprodukte für 2017, ebenfalls ohne Dienstleistungen einzuberechnen. Aber auch die Anzahl der Mitarbeiter im eigenen Unternehmen, die sich mit Cybersicherheit beschäftigen, ist nicht zu unterschätzen. Bei den DAX-Unternehmen sind das im Schnitt 131 Mitarbeiter, auch hier ca. 0,1 % der Mitarbeiter insgesamt.

Laut Prognosen der Credit Suisse lagen die weltweiten Ausgaben für Cybersicherheit 2017 bei 135 Milliarden US-Dollar und werden 2021 etwa 202,4 Milliarden US-Dollar erreichen. Damit ist das prognostizierte Wachstum durchschnittlich 10% im Jahr. Dieser Wachstumswert ist höher als der prognostizierte für IT-Ausgaben als Ganzes. Damit werden die Ausgaben für Cybersicherheit schneller wachsen als die restlichen IT-Ausgaben.

Europa hat in den letzten Jahren sehr viel Energie in die Gesetzgebungen im Bereich der IT-Sicherheit und des Datenschutzes investiert. Die Datenschutz-Grundverordnung (DSGVO), die Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS) und die Richtlinie für Bezahldienste - Payment Services Directive (PSD2) sind einige Beispiele. Außerdem werden an der e-Privacy-Verordnung sowie an einem Cybersecurity Act gearbeitet. Auch wenn die Cybersicherheitsindustrie Regulierungen nicht gut finden, werden dadurch

Mining-Farmen für Kryptowährungen: Um die rechintensiven Prozesse zu bewältigen, nutzen Hacker auch die Computer unwissender Nutzer.

Foto: Blind



DIE CYBERSECURITY-MARKTFÜHRER IM BEREICH DER MASSENPRODUKTE, WIE ANTI-MALWARE, AUTHENTIFIZIERUNGS-LÖSUNGEN, FIREWALLS KOMMEN AUS DEN USA.

Standards in Europa etabliert, die den Cybersicherheitsmarkt in Europa deutlich stärken und Chancen für den weltweiter Cybersicherheitsindustrie eröffnen.

Die Cybersecurity-Marktführer im Bereich der Massenprodukte, wie Anti-Malware, Authentifizierungslösungen, Firewalls und anderen Produkten kommen aus den USA. Die deutschen Anbieter sind stark fragmentiert, bietet aber höherwertige Cybersicherheitslösungen wie Verschlüsselung, PKIs, proaktive Sicherheitssysteme und Hardwaresicherheitsmodule an. Im Bereich Expertise im Hochschul-, Forschungs- und Industriebereich spielt Deutschland an der Spitze mit und hat ideale Voraussetzungen, sich in der Cybersicherheit weiter erfolgreich zu positionieren.

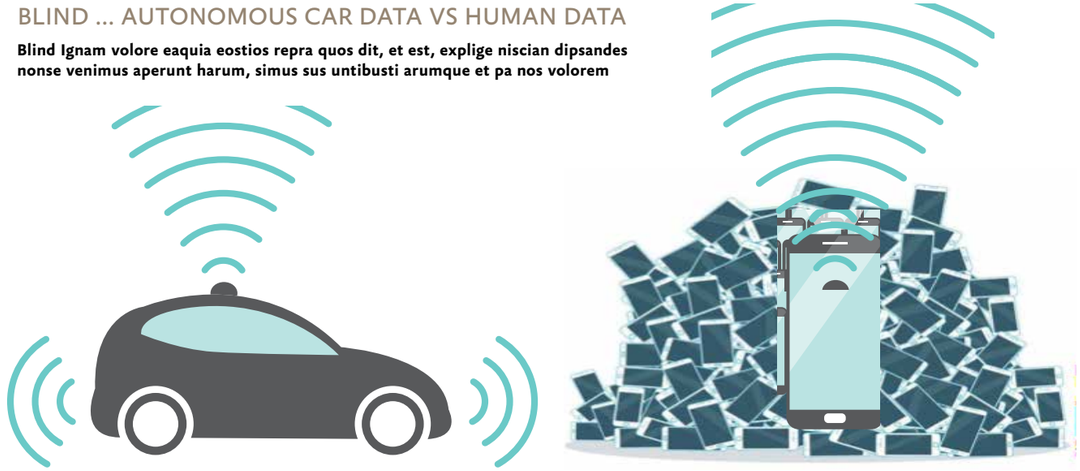
Bereits heute stehen sich ausgeklügelte Cybersicherheitslösungen und immer professioneller werdende Angreifer gegenüber. Im Hinblick auf die Zukunft werden wir deshalb mehr Sicherheit benötigen und es stellt sich die Frage, welche Innovationen notwendig sind, um den Risiken wirkungsvoll zu begegnen, damit die Digitalisierung nachhaltig sicher und vertrauenswürdig umgesetzt werden kann. Dabei zeichen sich folgende Paradigmenwechsel ab:

Paradigmenwechsel „Cloud-Service versus Lokal IT“: Eine vollständige Cloudifizierung im Gegensatz zur heutigen nur teilweisen Nutzung von Cloud-Diensten wird sich durchsetzen. Es ist keine Frage von „ob in die Cloud“, sondern lediglich „wann“ und bei diesem Prozess spielen Cybersicherheitslösungen für die Cloud eine wichtige Rolle. Das vergleichsweise mittelmäßige gegenwärtige IT-Sicherheitslevel bedarf deutlicher Verbesserung, um die Daten der Unternehmen angemessen schützen zu können.

Paradigmenwechsel „Proaktive versus reaktive Cybersicherheitslösungen“: Bei den heutigen reaktiven Cybersicherheitssystemen, wie Anti-Spam-, Anti-Malware-, Intrusion-Detection-Systemen rennen wir den IT-Angriffen hinterher. Das bedeutet, wenn die Cybersicherheitslösungen einen Angriff durch eine entsprechende Angriffssignatur oder eine Anoma- ›

BLIND ... AUTONOMOUS CAR DATA VS HUMAN DATA

Blind Ignam volore eaquia eostios repra quos dit, et est, explige niscian dipsandes nonse venimus aperunt harum, simus sus untibusti arumque et pa nos volorem



Digitale Trends: Allein die produzierte Datenmenge eines einzigen autonomen Autos entspricht etwa 2.666 Internetnutzern

lie erkennen, dann versuchen sie, uns so schnell wie möglich zu schützen, um den Schaden zu reduzieren. Die zunehmende Vielfalt und Komplexität unserer IT-Systeme und IT-Infrastrukturen brauchen aber verlässlichere, robustere und wirkungsvollere IT-Sicherheitskonzepte. Wir müssen weg von ausschließlich reaktiven hin zu modernen proaktiven Cybersicherheitssystemen, die eine Ausführung von intelligenter Malware, eines der größten Probleme zurzeit, verhindern können. Solche proaktiven Cybersicherheitssysteme arbeiten mit einem kleinen Sicherheitskern (sichere Betriebssysteme) und Virtualisierung, können Software messbar machen und mit einer starken Isolation Anwendungen mit ihren Daten separieren und so nachhaltige und angemessene Cybersicherheit bieten.

Paradigmenwechsel „Dezentrale versus zentrale Cybersicherheit“: Statt aufwendige zentrale Cybersicherheitslösungen wie PKIs, werden für die automatisiert vertrauenswürdige Zusammenarbeit verschiedener Unternehmen dezentrale Cybersicherheitslösungen immer wichtiger. Die Blockchain-Technologie stellt ein „programmiertes Vertrauen“ zur Verfügung, weil alle IT-Sicherheitseigenschaften als Security-by-Design inhärent in der Blockchain-Technologie eingebunden sind. Die Blockchain-Technologie schafft eine Grundlage für verteilte und vertrauenswürdige Zusammenarbeit und hat ein hohes Potenzial für neue Geschäftsmodelle und Ökosysteme.

Paradigmenwechsel „Objekt-Sicherheit versus Perimeter-Sicherheit“: Perimeter-Sicherheit soll z.B. mit Hilfe von Firewall- und VPN-Systemen verhindern, dass Fremde aus dem Internet auf das eigene Unternehmensnetz zugreifen können und, dass die ausgetauschten Daten nicht von anderen gelesen und manipuliert werden können. Da aber immer mehr mobile Geräte über alternative Kommunikationswege, wie Mobilfunknetze und Hotspots, vorbei an der zentralen Unternehmens-Firewall ins Internet gehen, verliert die Perimeter-Sicherheit an Wirkung und Bedeutung. Bei Objekt-Sicherheit, Informationsflusskontrolle werden die Objekte mit Rechten versehen, die definieren, wer sie in welcher IT-Umgebung wie nutzen darf. Die Objekte werden dadurch über ihren ganzen Lebenszyklus vertrauenswürdig gesichert.

Paradigmenwechsel „Daten-getriebene- versus Event-getriebene-Sicherheit“: Heute versuchen wir überwiegend über identifizierbare Events Angriffe zu erkennen. Zukünftig werden wir mit Hilfe Künstlicher Intelligenz aus immer mehr vorhandenen Daten sicherheitsrelevante Informationen extrahieren, die helfen, für mehr Cybersicherheit zu sorgen. Data Science mit Technologien des Maschinellen Lernens und Künstlicher Intelligenz verspricht Innovationen bei der Erkennung von Angriffen, neben vielen anderen wichtigen Aspekten wie Authentifizierung oder Threat Intelligence im Bereich der Cybersicherheit.

IT und Internet gehören zu den Schlüsselkomponenten unserer modernen Gesellschaft. Daten stellen zunehmend das Kapital von Unternehmen dar. Mit Hilfe moderner, sicherer und vertrauenswürdigerer Sicherheitslösungen muss für eine verlässliche Nutzung gesorgt werden. Aus diesem Grund bekommt die Cybersicherheitsindustrie eine immer größer werdende ökonomische Relevanz. //

NORBERT POHLMANN

GELSENKIRCHEN 51° 31′ N, 7° 6′ O

Der Autor ist Professor für Verteilte Systeme und Informationssicherheit an der Westfälischen Hochschule Gelsenkirchen. ist Pohl-