Bundesamt für Sicherheit
in der Informationstechnik
Bundesamt für Verfassungsschutz
Bundeskriminalamt
Bundesnachrichtendienst

Sonderbericht Wirtschaftsschutz

Informationen der deutschen Sicherheitsbehörden des Bundes

1. Sonderausgabe Cybersicherheit

Stand: 01.12.2014

Inhaltsverzeichnis

1. Deutschland: Vorwort zur 1. Sonderausgabe Cybersicherheit

Beim letzten Treffen der Redaktionskonferenz des Sonderberichtes Wirtschaftsschutz beschlossen die beteiligten Behörden BKA, BSI, BfV und BND die Einführung eines neuen Formats des Sonderberichtes: die vorliegende Sonderausgabe Cybersicherheit. Damit soll der zunehmenden Bedeutung dieses Themas Rechnung getragen werden. In der Anfang 2014 durchgeführten Umfrage unter den Lesern des Berichts wurde insbesondere das Thema „Cyber“ als Interessensschwerpunkt genannt. Die Sonderausgabe Cybersicherheit wird in unregelmäßigen Abständen bei Vorliegen von vier bis fünf geeigneten Beiträgen bei den Behörden erscheinen.

Das Internet ist ein unverzichtbarer Teil der gesellschaftlichen Interaktion und der Wertschöpfungskette geworden. So ist beispielsweise die Lösung hochkomplexer logistischer Aufgaben des Transportwesens oder von Produktionsprozessen der Industrie ohne das Internet nicht mehr denkbar. Auch staatliche Verwaltungsprozesse sind zunehmend auf dieses Medium angewiesen. Durch das „Internet der Dinge“ tauchen Bereiche auf, die vor wenigen Jahren noch Fiktion waren. So sind nicht nur die häusliche Energieversorgung, sondern auch Kühlschränke und Kraftfahrzeuge aus dem Internet erreichbar. Deshalb ist die heutige Lebensqualität gefährdet, wenn wesentliche Funktionen und Dienstleistungen im Internet ausfallen. Aus diesem Grunde stellt der Cyber-Raum als Abstraktion des über das Internet verwobenen globalen Datenbestandes eine ausgesprochen wichtige, zu schützende Ressource dar.

Cyber-Angriffe gegen die deutsche Wirtschaft, Industrie und Regierungsstellen haben in den letzten Jahren einen deutlichen Anstieg erfahren. Hier unterscheiden wir hauptsächlich zwischen Angriffen durch kriminelle Hacker, welche meist auf einen finanziellen Gewinn abzielen und Akteuren, die im Auftrag einer ausländischen Regierung agieren. Bei den staatlich motivierten Cyber-Angriffen handelt es sich entweder um Cyber-Spionage mit dem Ziel der Erlangung von nicht frei zugänglichen Informationen, oder um Cyber-Sabotage, welche auf eine Störung der Funktionsfähigkeit von Netzwerken oder Computern abzielt.

In Fällen deutscher Betroffenheit arbeiten die Sicherheitsbehörden BfV, BSI, BKA und BND sehr eng zusammen. Beispielsweise verfügt der BND als nationale SIGINT-Behörde über die Fähigkeit zur strategischen Erfassung internationaler Datenverkehre zur Cyber-Abwehr: SIGINT Support to Cyber Defence - kurz SSCD. Durch eine

Identifizierung von Schadsoftware-Aktivitäten in den Datenströmen des Cyber-Raumes können Cyber-Angriffe in Echtzeit erkannt und Schäden verhindert werden.
Mit dem Start der „Sonderausgabe Cyber-Sicherheit“ informieren die Sicherheitsbehörden über aktuelle Cyber-Bedrohungen, welche für die Privatwirtschaft von besonderem Interesse sein dürften. (BND, BSI)

2. Deutschland: E-Mail als größter Angriffsvektor für Schadsoftware-Infektionen

Ein beliebtes Mittel zur Initialisierung von Cyber-Angriffen sind nach wie vor E-Mails. Diese beinhalten häufig einen Anhang mit oder einen Download-Link auf Schadsoftware, die – ein-mal angeklickt – dem Täter vielfältige Möglichkeiten eröffnen. Das BSI detektiert beim Scan der an deutsche Behörden gesendeten E-Mails immer wieder derartige Angriffsversuche. Auch aus der Wirtschaft werden regelmäßig Angriffswellen gemeldet. Mit wenigen gezielten Maßnahmen lässt sich die Gefahr jedoch deutlich reduzieren.

Im September 2014 lag der Anteil der Spam-E-Mails am gesamten Online-Schriftverkehr bei über 80 Prozent. Zwischen den hinlänglich bekannten Werbe-Mails für fragwürdige Medikamente und unseriöse Liebesdienste verbargen sich auch immer wieder Anhänge, die beim Ausführen durch den Mail-Empfänger eine Schadsoftware auf dessen Rechner installierten. Ebenfalls wurde in einigen Mails auf Webseiten verlinkt, die beim Aufruf durch den Nutzer eine Malware-Infektion zur Folge hatten (Drive-by-Download). Neben diesen so genannten Flächenangriffen, bei denen die Täter versuchen, wahllos Systeme zu kompromittieren, sind aber auch immer mehr gezielte Angriffe per E-Mail zu beobachten: Cyber-Kriminelle verfassen speziell auf die Opfer zugeschnittene Mails und fälschen die Absenderadresse so, dass beim Empfänger der Eindruck erweckt wird, es handle sich um eine integre Zusendung – zum Beispiel eines Kollegen oder Kunden – die bedenkenlos geöffnet werden kann.

Auch Mitarbeiter deutscher Behörden erhielten in den vergangenen Monaten vermehrt gut getarnte E-Mails mit Angriffsabsicht. So meldeten mehrere Behörden im Frühjahr dieses Jahres den Eingang von gut gestalteten, gefälschten eFax-Nachrichten – ein Dienst, der im Auftrag seiner Kunden Fax-Sendungen in E-Mails umwandelt. Bei den Nachrichten handelte es sich jedoch um Spam-Mails, die jeweils einen Link auf ein ZIP-Archiv mitlieferten, das wiederum eine infizierte Datei einem Schadprogramm

enthielt. In diesen E-Mails wird dem Empfänger vorgetäuscht, dass für ihn ein elektronisches Fax eingegangen sei. Das Fax könne auf der Seite des tatsächlich existierenden Dienstleisters „eFax“ betrachtet werden. Erst eine nähere Betrachtung des vermeintlichen Fax-Links zu efax.com zeigt, dass der Link zu einer anderen Webseite führt. Dort ist das ZIPArchiv mit dem enthaltenen Schadprogramm abgelegt. Da es sich bei der eFax-Ankündigung um eine HTML-E-Mail und nicht um eine reine Text-E-Mail handelt, fällt der Schwindel beim flüchtigen Betrachten nicht direkt auf. In den gemeldeten Fällen enthielt das ZIP-Archiv mit dem Namen „pdf_efax_<NummerCallerID>.zip“ eine gleichnamige unter Windows ausführbare PIF-Datei, die das später eingesetzte Schadprogramm nachlädt.

Die Erkennungsrate der verlinkten Schadprogramme durch Antiviren-Programme war zum Empfangszeitpunkt der E-Mail in den gemeldeten Fällen mit etwa 10 Prozent relativ gering. Die Kampagne mit den vermeintlichen eFax-Nachrichten war glaubwürdig gestaltet. Gerade in Sekretariaten, die vielfach die erste Anlaufstelle für Korrespondenz und elektronische Fax-nachrichten sind, führte dies dazu, dass das verlinkte ZIP-Archiv geöffnet und das enthaltene Schadprogramm ausgeführt wurde. Da die Schadprogramm-Spam-Nachrichten massenhaft verbreitet wurden, ist bei den gefälschten eFax-Nachrichten nicht von zielgerichteten Angriffen auszugehen. Weil das ZIP-Archiv nicht direkt als Anhang beigefügt war, sondern nur per Link darauf verwiesen wurde, dürfte die E-Mail in vielen Fällen ohne weitere Spam-Markierung den Posteingang der Empfänger erreicht haben.

Das Computer-Notfallteam des Bundes, CERT-Bund, hat für die angebundenen Behörden in den gemeldeten Fällen die gefährlichen Links aus den E-Mails zeitnah im behördeninternen Schadsoftware-Präventions-System aufgenommen, um ein Herunterladen durch weitere Benutzer zu verhindern. Des Weiteren erhielten die Hosting-Unternehmen, die die Webseite mit dem Schadprogramm lagerten, eine entsprechende Mitteilung. Da die genannten technischen Maßnahmen nicht immer in

jeder Organisation durchgeführt werden können, hat sich die Sensibilisierung von Mitarbeitern für Cyber-Gefährdungen in der Vergangenheit als adäquates Mittel zum Schutz erwiesen: Wer umsichtig mit E-Mails und anderen Online-Angeboten umgeht und sich der Gefahren bewusst ist, kann die Wahrscheinlichkeit einer Infektion mit Malware durch sein eigenes Verhalten deutlich reduzieren. Aus diesem Grund empfiehlt es sich, neben den obligatorischen technischen Schutzmaßnahmen auch regelmäßig Mitarbeiterschulungen in IT-Security-Awareness durchzuführen. In der jüngeren Vergangenheit sind hierfür immer neue Angebote erschienen, wie bspw. Schulungsunterlagen oder Lernspiele. Bereits mit geringem Aufwand lässt sich das Bewusstsein für Cyber-Bedrohungen so signifikant erhöhen. (BSI)

3. Deutschland: Industrieanlagen im Fokus der Angreifer

Systeme zur Fertigungs- und Prozessautomatisierung (Industrial Control Systems, kurz ICS) sind zunehmend denselben Bedrohungen aus dem Cyber-Raum ausgesetzt wie die konventionelle IT. Die Betreiber müssen sich angesichts der Zunahme von Vorfällen und neu entdeckten Schwachstellen dringend dieser Thematik annehmen. So müssen Risiko und Schadenspotenzial sowohl von nicht-zielgerichteter Schadsoftware als auch von gezielten, qualitativ hochwertigen und mit signifikantem Aufwand durchgeführten spezifischen Angriffen gegen ICS-Infrastrukturen berücksichtigt werden. Dies gilt sowohl für Infrastrukturen, die unmittelbar mit dem Internet verbunden sind, als auch für diejenigen, welche auf mittelbarem Wege durch Cyber-Angriffe attackiert werden können.

Steuerungskomponenten sind heute nicht nur in mittelständischen Produktionsanlagen, sondern auch bei global tätigen Konzernen oder Installationen der öffentlichen Verwaltung im Einsatz. Cyber-Angriffe beispielsweise auf Kühlanlagen von Atomkraftwerken oder Verkehrsleitsystemen in Ballungsräumen können daher schnell zur Gefahr für das Gemeinwohl werden.

Um die Sicherheit dieser Anlagen zu optimieren, arbeitet das BSI bereits seit geraumer Zeit mit verschiedenen Betreibern zusammen und erhält dadurch regelmäßig aktuelle Hinweise zu Angriffsversuchen. Im Rahmen dieser Kooperation wurde dem BSI auch ein Angriff auf ein Stahlwerk in Deutschland gemeldet. Mittels ausgefeilter Spear-Phishing und Social Engineering-Methoden – bspw. durch das gezielte Anschreiben von Mitarbeitern mit raffiniert gefälschten E-Mails, die den Empfänger wahlweise zur

Eingabe von Zugangsdaten oder zum Herunterladen einer Schadsoftware verleiten sollen – gelang es den Angreifern, Zugriff auf das Büronetz des Stahlwerks zu erhalten. Von dort aus konnten sie sich anschließend bis in die Produktionsnetze vorarbeiten. Für das Stahlwerk hatte dies massive Schäden an den Produktionsanlagen zur Folge: Zunächst kam es zu einer auffälligen Häufung von Ausfällen einzelner Steuerungskomponenten oder ganzer Anlagen. Diese führten dazu, dass die Mitarbeiter den Hochofen weder geregelt herunterfahren noch vollständig kontrollieren konnten.

Der Vorfall zeigt exemplarisch, dass Wissen und Professionalität von Cyber-Angreifern in den vergangenen Jahren stark zugenommen haben. Zu einem derartigen Angriff auf eine Produktionsanlage ist mehr als reines Know-how zu klassischen IT-Komponenten notwendig – vielmehr waren in dem Produktionsnetz Steuerungskomponenten, Sensoren und Aktoren im Einsatz. Um die zielführenden Komponenten angreifen und den Hochofen somit beschädigen zu können, müssen die Täter also über detailliertes Fachwissen verfügt haben.

Das Beispiel beinhaltet in vielerlei Hinsicht die aktuellen Top-Bedrohungen, denen das BSI die höchste Kritikalität für ICS-Angriffe zuschreibt[1]:

1. Infektion von Steuerungskomponenten mit Schadsoftware über Büronetze
2. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3. Social Engineering
4. Menschliches Fehlverhalten und Sabotage
5. Einbruch über Fernwartungszugänge

Bei dem vorliegenden Stahlwerkvorfall wurden nahezu alle unter den Top-Bedrohungen genannten ausgenutzt: Per Social Engineering (3) wurden die Mitarbeiter dazu verleitet, Schadsoftware zu installieren bzw. Kennwörter preiszugeben (1, 4). Anschließend war es den Angreifern möglich, aus der Ferne auf das kompromittierte Netz zuzugreifen (5). Im Zuge der weiter steigenden Vernetzung von Industrieanlagen und ganzen Unternehmen weltweit „Industrie 4.0“, ergeben sich für die Zukunft weitere Bedrohungsszenarien von heute noch nicht abschätzbarem Ausmaß. Aufgrund dessen gilt es, Anlagenbetreiber frühzeitig über Cyber-Bedrohungen aufzuklären und diese bei der Einführung von IT-Sicherheitsmaßnahmen umfassend zu unterstützen.

[1] Vollständige Beschreibung der Bedrohungen und Lösungsansätze im Dokument „Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2014“ https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/ techniker/hardware/BSI-CS_005.html.

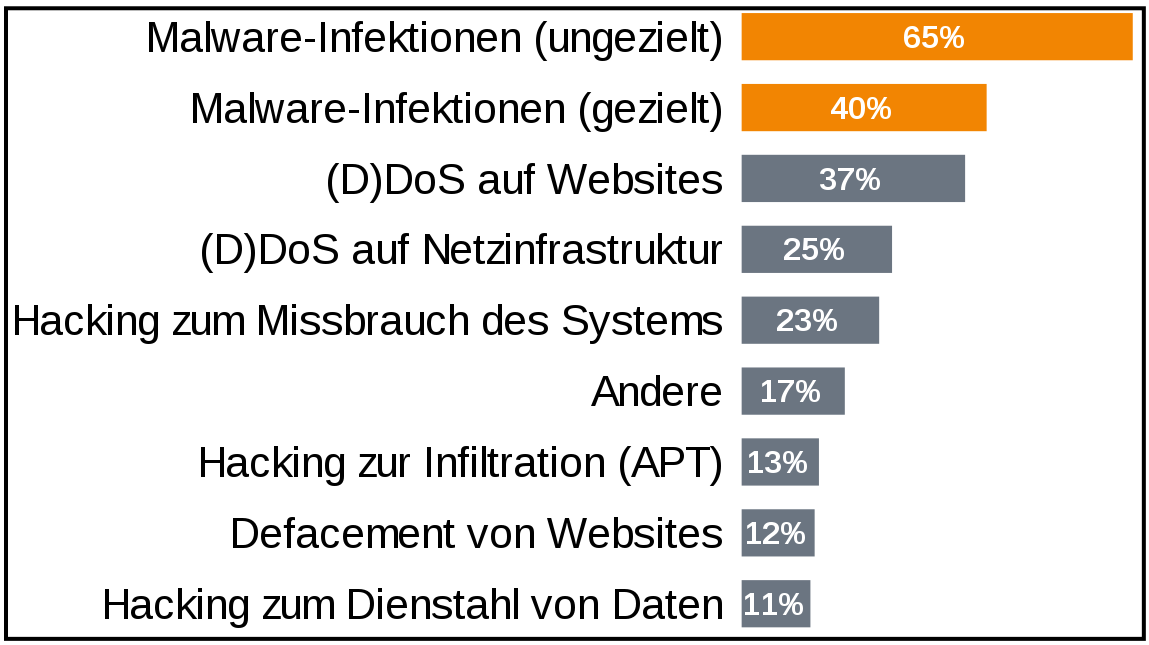
Während für Bestandsanlagen eine meist überschaubare Menge an Sicherheitsmechanismen genügt, um ein hinreichendes Sicherheitsniveau zu erreichen, müssen für „Industrie 4.0“ neue Konzepte erarbeitet werden. In erster Linie gilt es, die mit einer „Industrie 4.0“ aufgrund der starken Vernetzung einhergehende Komplexität der Systeme beherrschbar zu machen. Die klassische Herangehensweise der Segmentierung und minimalen Kopplung von unterschiedlichen Teilnetzen in der Automatisierungspyramide wird dabei nicht mehr funktionieren. Zudem sehen viele Szenarien für „Industrie 4.0“ eine unternehmensübergreifende Vernetzung entlang der gesamten Wertschöpfungskette vor. Diese Entwicklung erfordert, umfassende und dezentralisierte Konzepte für das Management von Identitäten, Rollen und Berechtigungen zu etablieren. Ein händisches Etablieren statischer Vertrauensbeziehungen wird mit „Industrie 4.0“ nicht mehr praktikabel sein. So werden Technologien für die Bildung von Vertrauensankern für Prozesse in der „Industrie 4.0“ eine wichtige Rolle spielen. Sicherheit darf zudem nicht zu kostspielig für den Anlagenbetreiber werden, weshalb das Thema „Security by Design“ zur Bewältigung von Herausforderungen wie der Patch-Problematik in Industrieanlagen von besonderer Relevanz ist. Auch bedarf es neuer Basistechnologien zur sicheren und vertrauenswürdigen Kommunikation. Neue, mit sicherheitsspezifischen Funktionen angereicherte Standards, wie beispielsweise OPC UA, werden hier zukünftig unabdingbar sein. (BSI)

4. Deutschland: Umfrage sieht Unternehmen zunehmend im Fokus von Cyber-Bedrohungen

In den vergangenen drei Jahren war bereits jedes zweite Unternehmen Ziel von Cyber-Angriffen; jedes vierte Unternehmen hat durch einen Cyber-Angriff einen Schaden erlitten. Dies sind die zentralen Ergebnisse der Cyber-Sicherheits-Umfrage 2014, die von der Allianz für Cyber-Sicherheit beauftragt wurde und an der sich 257 Unternehmen, Behörden und weitere Einrichtungen branchenübergreifend beteiligten. Unterstützt wurde die Befragung durch den Bundesverband der Deutschen Industrie (BDI), den Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) sowie die Verbände der IT-Anwender (VOICE) und des Zentralverbands Elektrotechnik- und Elektronikindustrie (ZVEI).

Die Ergebnisse der aktuellen Umfrage der Allianz für Cyber-Sicherheit verdeutlichen, dass Cyber-Angriffe und die resultierenden Folgeschäden inzwischen Realität sind. Im

Hinblick auf die Angriffsarten stellen Flächenangriffe, wie Malware-Infektionen mittels Spam oder Drive-by-download, die häufigsten erkannten Cyber-Angriffe dar. Daneben wurden bei den befragten Unternehmen zahlreiche gezielte, vorsätzliche Cyber-Angriffe (DDoS, Hacking) detektiert, mit denen Spionage, Sabotage, Erpressung oder Datenmissbrauch und -diebstahl durchgeführt werden können. Die genannten Angriffsarten können bei kleinen und mittelständischen Unternehmen schnell zu gravierenden wirtschaftlichen Schäden führen. Auch Behörden und andere Institutionen können durch erfolgreiche Spionage und Datenabfluss stark geschädigt werden.



Genannte Arten von Cyber-Angriffen in Prozentzahl

Durch die immer professioneller agierenden Cyber-Angreifer nehmen Betroffenheit und Verletzbarkeit der Betriebsfähigkeit von Unternehmen deutlich zu. Für drei Viertel der befragten Institutionen stellen Cyber-Angriffe bereits eine relevante Bedrohung der Betriebsfähigkeit dar. Die Befragten sehen sich mittelfristig vor allem durch Cyber-Kriminelle bedroht. Trotz der weiterhin aktuellen Medienberichterstattung um die Ausspäh-Aktivitäten des US-Geheimdienstes NSA schätzt lediglich die Hälfte der Befragten staatliche Angreifer als relevante Bedrohung ein. Mit nur einem Fünftel gaben relativ wenige Befragte an, Hacktivismus als Bedrohung in die unternehmenseigene Risikoabschätzung mit einzubeziehen. So vielschichtig wie die Motivation der Angreifer stellen sich auch die Gründe dar, auf die die Unternehmensverantwortlichen den Erfolg der Täter zurückführen. Bei der Hälfte der erfolgreichen Angriffe konnten Software-Schwachstellen ausgenutzt werden, in knapp vierzig Prozent der Fälle handelte es sich um die besonders gefährlichen Zero-day-Exploits, für die zunächst keine Patches zur Verfügung stehen. Zu jeweils einem Drittel

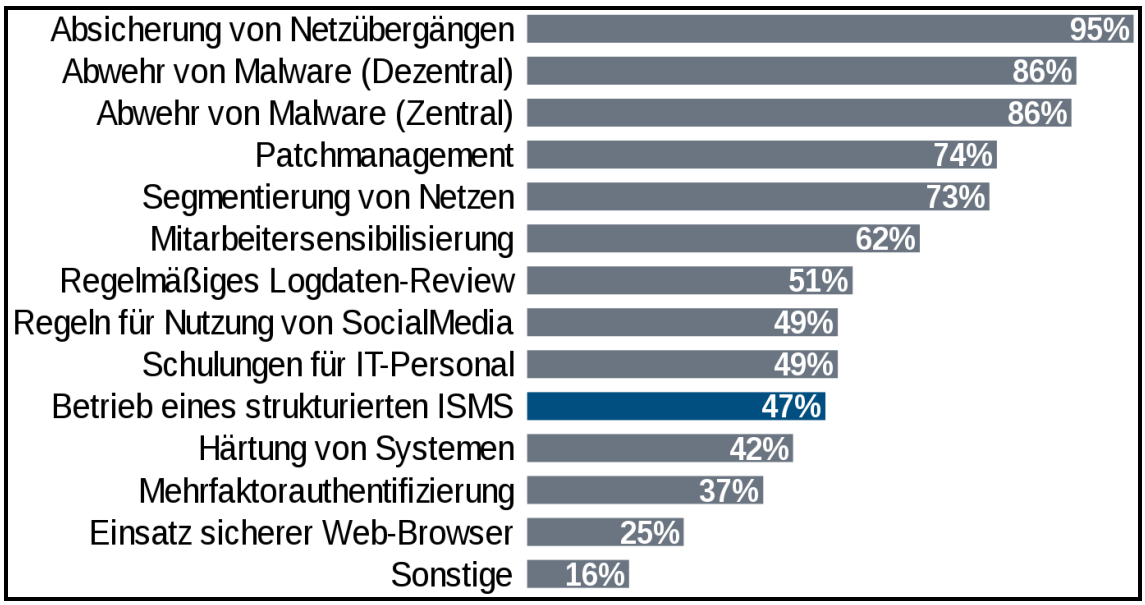
konnten erfolgreiche Angriffe auf unzureichend gesicherte Systeme durch eigene Mitarbeiter und durch unbeabsichtigtes Fehlverhalten von Mitarbeitern erfolgen. Mittels erfolgreichem Social Engineering wurden zudem Mitarbeiter angesprochen und Sicherheitsvorkehrungen überwunden.

Unternehmen, die bereits von einem Cyber-Angriff betroffen waren, wurden am stärksten durch erhebliche Kosten für die Aufklärung und Wiederherstellung der Systeme geschädigt. Dahinter folgten der erlittene Reputationsschaden sowie Produktionsausfälle. Stark getroffen wurden die Firmen auch durch den Diebstahl digitaler Identitäten mittels derer sich Unbefugte Zugriff auf sensible Unternehmensdaten verschaffen können. Auch Informationsabfluss, zum Beispiel von Entwicklungsdaten, wurde mehrfach als Schaden angegeben. Die Befragten gehen davon aus, dass für ihr Unternehmen in den kommenden zwei Jahren die größte Gefahr von der Organisierten Kriminalität ausgeht, gefolgt von Wirtschaftskriminellen, staatlichen Angreifern und Hackern.

Ein erfreuliches Ergebnis der Umfrage ist, dass es inzwischen Unternehmen gibt, die IT- und Cyber-Sicherheit schon hoch priorisieren und die notwendigen technischen, organisatorischen und personellen Maßnahmen ergreifen, um die Sicherheit ihrer Systeme und Daten gewährleisten zu können. Die für die Cyber-Sicherheits-Umfrage befragten Unternehmen geben vielfältige Maßnahmen an, die sie bereits ergreifen. Am weitesten verbreitet ist die Absicherung von Netzübergängen, beispielsweise mit Sicherheitsgateways oder Firewalls. Hinzukommt eine dezentrale Abwehr von Schadprogrammen mittels Antiviren-Software auf Client- und Serversystemen sowie eine zentrale Abwehr durch einen Antiviren-Scan am Sicherheitsgateway oder Mailserver. Ein großer Teil gab ebenfalls an, ein Patchmanagement installiert zu haben.

Die Umfrage bildet die aktuelle Situation – Bedrohungslage auf der einen und Unternehmen im Fokus der Angreifer auf der anderen Seite – gut ab. Die Gefährdungssituation wird stetig bedrohlicher, die Angreifer warten in immer kürzeren Zeitabständen mit immer schlechter zu detektierenden Angriffen auf, während sich die möglichen Opfer teilweise noch zu sehr in Sicherheit wähnen. Zwar hat sich in puncto IT- und Datensicherheit bereits einiges bewegt, aus Sicht des BSI sind Cyber-Angriffe und ihre Folgeschäden jedoch schon heute Realität, die daher unerlässlicher Bestandteil des Risikomanagements sein müssen. Durch professionelle Cyber-Angriffe steigt die Gefahr von Produktionsausfällen für Unternehmen: In 75 Prozent der befragten Institutionen stellen Cyber-Angriffe eine relevante Bedrohung der Betriebsfähigkeit dar. Notfallvorsorge und Business-Continuity-Management sind

daher als essentielle Bestandteile des Informationssicherheitsmanagements von Anfang an mit einzuplanen.



Maßnahmen zum Schutz gegen Cyber-Angriffe, die Befragte ergreifen wollen (Mehrfachnennungen möglich)

Die Bedrohungslage entwickelt sich konstant dynamischer: Bereits jedes zweite Unternehmen der Umfrage wurde schon Ziel von Cyber-Angriffen. Stetiger Austausch und aktuelle Information sind heute unerlässlich, um bei der sich schnell verändernden Bedrohungslage den Überblick behalten und die unternehmenseigenen Systeme adäquat schützen zu können. Die Allianz für Cyber-Sicherheit bietet mit einer Meldestelle einen wertvollen Kontakt, um Informationen zu Sicherheitsvorfällen – auch anonym – an das BSI zu übermitteln. Diese können dazu beitragen, frühzeitig neue Bedrohungen zu identifizieren und Unternehmen und Behörden zu warnen. Die Erkenntnisse fließen zudem in IT-Lagebilder ein. Die Allianz für Cybersicherheit und ihre inzwischen 1.000 Mitglieder leisten damit einen wichtigen Beitrag für die Cyber-Sicherheit in Deutschland. (BSI)

5. International: Cyber-Bedrohungen gegen Kraftfahrzeuge

Umweltanforderungen, Erhöhung der Unfallsicherheit und des Komforts führen zu einer immer komplexer werdenden vernetzten elektronischen Ausstattung von Kraftfahrzeugen. So sind alle modernen Fahrzeuge mit Bussystemen ausgerüstet, welche die Übertragung von Daten der Sensoren und von Anweisungen für die Stellelemente übernehmen. Kontrolliert wird dieses Zusammenspiel durch Steuergeräte. Die dadurch vorhandenen Schnittstellen ergeben eine Vielzahl von Angriffsmöglichkeiten sowohl für Cyber-Spionage als auch für Cyber-Sabotage. Entsprechend gestaltet sich auch die Bandbreite der möglichen Akteure – von staatlichen Organisationen bis hin zu Hackern.

Die Auswirkungen von Cyber-Angriffen auf Kraftfahrzeuge können vom einfachen Informationsabgriff bis hin zur empfindlichen Störung für die Verkehrsinfrastruktur oder das gezielte Auslösen von Unfällen geartet sein. Dennoch sind Cyberangriffe auf Fahrzeuge nicht ganz so leicht zu realisieren wie derzeit Angriffe auf Computer oder Mobiltelefone. Das liegt hauptsächlich daran, dass die Systeme in Fahrzeugen sehr vielfältig sind und der zu erbringende Aufwand für die Vorbereitung eines Erfolg versprechenden Angriffs noch vergleichsweise hoch ist.

In Fahrzeugen kommen verschiedene Bus-Systeme[2] zur Anwendung (CAN-BUS[3], LIN-BUS[4] und MOST-BUS[5]). Sie sind jeweils für bestimmte, spezifische Aufgaben optimiert. Ein Gateway[6], verbindet die Bus-Systeme miteinander. Hinzu kommen fahrzeuginterne Funknetzwerke – Bluetooth (Freisprechanlagen bzw. Audiostreaming), oder die Funkanbindung von Reifendrucksensoren. Moderne Fahrzeuge sind nicht nur intern vernetzt, sondern werden dahin gehend entwickelt, auch untereinander, mit Verkehrsleitsystemen oder durch die Service-Netzwerke der Hersteller, Verbindung aufzunehmen. Zwischen den vernetzten Komponenten gibt es deshalb eine ganze Reihe von Schnittstellen mit unterschiedlich starkem Missbrauchspotential. Je nach Art der Schnittstelle kann auch ein physikalischer Zugriff auf das Fahrzeug erforderlich sein

---

[2] Ein Bussystem dient der Datenübertragung zwischen mehreren Teilnehmern über einen gemeinsamen Übertragungsweg.

[3] CAN: Controller Area Network, ein serielles Bussystem.

[4] LIN: Local Interconnect Network, kostengünstiger Eindraht-Bus für die Anbindung intelligenter Sensoren und Aktoren in Kraftfahrzeugen.

[5] MOST: Media Oriented Systems Transport, ein Netzwerk zur Übertragung von Multimediadaten.

[6] Ein Gateway ist ein Vermittlungsgerät zwischen verschiedenen Rechnernetzen, welche mit unterschiedlichen Übertragungsprotokollen arbeiten.

(z.B. OBDII-Schnittstelle[7]), oder der Zugriff erfolgt über Funk (z.B. Infotainmentsysteme mit Bluetooth, WLAN, oder Mobilfunk).

Mögliche Angriffsvektoren unterscheiden sich daher in solche mit erforderlichem, direkten Zugriff auf das Fahrzeug und solche über Funkverbindungen. Direkte Zugriffe lassen sich über die OBDII-Schnittstelle, den CAN-BUS (z.B. über elektrisch verstellbare Außenspiegel oder Motorraum), über Schnittstellenerweiterungen des OBDII-Anschlusses durch WLAN, GSM oder Bluetooth, über als Multimedia-Dateien getarnte Malware auf Datenträgern für Infotainmentsysteme realisieren. Indirekte Zugriffe nutzen die Funkverbindungen des Fahrzeugs. Dabei wird der Anschluss des Multimediasystems an das Internet ausgenutzt. Diese Verbindung erfolgt mittels integriertem 3G/4G[8]-Modem oder durch Bluetooth- beziehungsweise WLAN-Tethering über das Mobiltelefon des Fahrzeugführers. Auch Schnittstellen, welche diverse Apps[9] zur Bedienung von Komfortfunktionen unter Nutzung des Internet (PC, Mobiltelefon, Tablet) verwenden, sind angreifbar. Sind die Schnittstellen zum Fahrzeug erst einmal zugänglich, können darüber sehr weitreichende Eingriffe sowohl in die Steuerung des Fahrzeugs, als auch zum Abgriff von Daten erfolgen.

Die sich ergebenden Gefahren sind abhängig von den jeweiligen Akteuren. Diese können sowohl staatliche Akteure, private Technikinteressierte, als auch Kriminelle sein. Die erforderlichen Informationen für die Einflussmahne auf den Datenverkehr des Fahrzeugbusses lassen sich überwiegend mit sogenannten „Sniffern“ gewinnen[10]. Die Methoden zur Erlangung der notwendigen Informationen werden nachvollziehbar im Internet publiziert. Davon profitieren auch Kreise mit kriminellen Absichten, denen auf diese Weise mehr oder weniger anwendungsbereite Lösungen zugänglich werden.

Folgende Szenarien können daher von den Akteuren ausgenutzt werden:

- Abschalten des Motors und damit Verhinderung des Antritts oder der Fortsetzung einer Fahrt
- Verhinderung des Antritts einer Fahrt durch Aktivierung der Wegfahrsperre
- Veränderung der Motordrehzahl im laufenden Betrieb (Beschleunigung / Verzögerung)

---

7 OBDII: On Board Diagnose II.

8 3G/4G: steht für 3. und 4. Generation der Mobilfunkstandards.

9 App: die umgangssprachliche Kurzbezeichnung für Anwendungssoftware bzw. Anwendungs-programm.

10 Sniffer sind Geräte die eine Aufzeichnung von Signalen zwischen Schnittstellen ermöglichen. Diese Aufzeichnungen können mit den beobachteten Aktionen des Kfz abgeglichen werden, um die Bedeutung einer Signalfolge festzustellen und sie gegebenenfalls zu kopieren.

- Manipulation des ABS-Regelkreises bis hin zum völligen Verlust der Bremsleistung
- Bei Fahrzeugen mit automatisch lenkenden Einparkhilfen das Provozieren von Lenkmanövern während der Fahrt
- Schalten der Fahrzeugbeleuchtung (z.B. unerwartetes Abschalten bei Dunkelheit)
- Bei Fahrzeugen mit Bremsassistenzsystemen das Auslösen von unerwarteten Bremsmanövern
- Aktivierung von Warnblinkanlage und Signalhorn
- Auslösen von Airbags

Die Absicht hinter einem Angriff auf ein Fahrzeugnetzwerk kann unterschiedlicher Natur sein. Im einfachen Fall werden nur Informationen abgerufen, die auf den Aufenthaltsort, die zurückgelegte Wegstrecke oder den Fahrstil des Fahrers schließen lassen (Cyber-Spionage). Auch das Aktivieren einer Wegfahrsperre aus der Ferne ist möglich. Gesammelte Informationen könnten Cyber-Kriminelle beispielsweise Versicherungen anbieten, um im Falle eines Schadeneintritts (Diebstahl) das Fahrzeug aufzufinden.

Angriffe, welche die Fahrsicherheit und damit die Verkehrsinfrastruktur als solches gefährden, sind dem Bereich der Cyber-Sabotage zuzuordnen. Dadurch können sowohl Personen zu Schaden kommen, als auch erhebliche wirtschaftliche Schäden entstehen.

Derzeit gibt es an Fahrzeugen keine technischen Lösungen, die ein nicht-autorisiertes Abgreifen von Daten zuverlässig verhindern. Folglich muss die Frage des Datenschutzes in Bezug auf die vielen, in einem Fahrzeug entstehenden und verarbeiteten Daten immer mehr einer kritischen Betrachtung standhalten. Hierbei sehen sich insbesondere die Fahrzeughersteller mit der Herausforderung konfrontiert, entsprechende Vorkehrungen und Regeln zur Verhinderung des Missbrauchs zu erarbeiten. (BND)