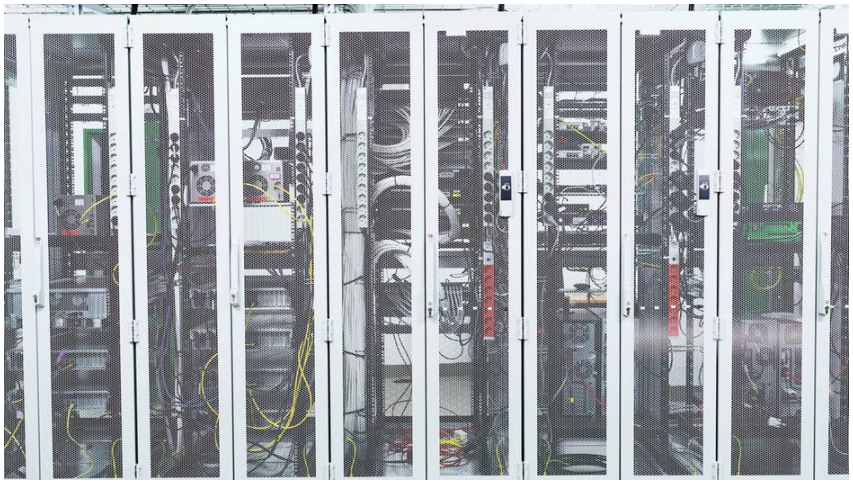
stern

Cyberkriminalität

03. August 2019 16:33 Uhr

Die digitale Front: So wappnet sich die Bundeswehr gegen Hacker-Angriffe

Die Schlachten der Zukunft werden im Internet geführt: Wahlmanipulationen, Datenklau, Attacken auf die Infrastruktur. Alles ist verwundbar. So schützen sich Bundeswehr, Unternehmen und Versorger



Früher reichten Zaun und Pförtner, heute hängt die Sicherheit der Berliner Wasserbetriebe von diesen Schränken ab

©Philipp von Ditfurth/stern

Ruben Rehage »

Redakteur im Hauptstadtbüro

» Zur Autorenseite

Die Front verläuft quer durch eine Kirche, mitten auf dem Luftwaffenstützpunkt Köln-Wahn, die Soldaten haben die Jalousien heruntergelassen, Red-Bull-Dosen stehen auf den Tischen, gerade hat es ein paar Würstchen gegeben, als um 13.42 Uhr eine Frau aufsteht und ruft: "Aufpassen! Wir werden angegriffen!"

Major Bernd Kammermeier kommt dazu, ein kleiner, etwas rundlicher Mann mit Glatze, er trägt Tarnhose, Bundeswehrstiefel. Er schaut der Soldatin über die Schulter und sagt: "Das ist schlecht. Wie lange sind die schon da?" "Das wissen wir nicht, heute Morgen war es schon komisch, wir konnten das nicht einordnen, jetzt sind die auf unserer Firewall."

"Was macht ihr jetzt?"

"Wahrscheinlich abschalten, komplett neu aufsetzen."

Kammermeier nickt.

Die Soldaten sitzen vor ihren Monitoren, tippen lange Zeilen Code auf schwarze Oberflächen.

Kammermeier sagt: "Die Jungs und Mädels hier sind die einzige Einheit der Bundeswehr, die permanent im Krieg ist." Sie gehören zum Kommando Cyber- und Informationsraum (CIR), der digitalen

Abwehreinheit der Bundeswehr. Gerade nehmen sie mit 44 Männern und Frauen an der internationalen Cyber-Abwehrübung "Locked Shields" teil, bei der 23 europäische Nationen und ein Team der Nato digitalen Krieg gegeneinander führen.

6 Billionen Dollar Schaden durch Cyberkriminalität

Bei dem Wort Krieg denkt man an Panzer, Luftangriffe, Artillerie und den Lärm von Gewehrsalven. Der Krieg, den Kammermeier und seine Kameraden führen, ist anders. Es ist ein alltäglicher Krieg, der, unabhängig von Locked Shields, jeden Tag stattfindet, im Digitalen, und dort an mehreren Fronten gleichzeitig, rund um die Uhr. Permanent wird die Bundesrepublik Deutschland angegriffen – und nicht nur die Bundeswehr, auch Unternehmen führen diesen Krieg gegen Angriffe aus dem Internet, die Versorger, die Politik, irgendwie ist jeder Bürger betroffen, auch wenn er davon gar nicht viel mitbekommt.

Major Bernd Kammermeier (r.) führt das deutsche Team bei der Cyberübung "Locked Shields"
©Martina Pump/Bundeswehr

Die meisten Angriffe tauchen nur in den Statistiken auf, werden automatisch abgefangen. Einige wenige aber haben das Potenzial, dramatischen Schaden anzurichten.

So griffen 2010 Hacker im Zuge der "Stuxnet"-Attacke mehrere iranische Industrieanlagen an und sabotierten die Systeme. Ende 2016 knipsten Hacker die Stromversorgung von Kiew aus. Zwei Beispiele, in denen Angreifer so systematisch vorgingen, so viel Zeit hatten, so viel Know-how, dass Experten vermuten: Es können nur Regierungen dahinterstecken.

Laut einer Studie der Herjavec-Gruppe, eines der anerkanntesten IT-Sicherheitsdienstleister der Welt, wird der Schaden durch Cyberkriminalität bis 2021 sechs Billionen Dollar jährlich betragen. Bisher blieb die Bundesrepublik einigermaßen verschont, ein paar Erpressungsversuche, ein paar Kinderzimmerhacker.

Bisher.

Sicher ist: Der Tag wird kommen, an dem es uns erwischt. Was dann passiert? Der Fantasie sind praktisch keine Grenzen gesetzt. Stromausfälle, riesige Datenleaks, Blackouts, manipulierte Wahlen. Man kann den Teufel an die Wand malen, und man kann sich sicher sein: Theoretisch ist das Szenario möglich.

Wie steht es also um unsere Sicherheit im Internet? Ist die Bundesrepublik digital abwehrbereit?

Kammermeier lächelt müde, als wollte er fragen: Wo soll ich anfangen?

Angriff auf das Wassernetz

Locked Shields ist eine Übung, es gibt ein Szenario, in dem der demokratische Inselstaat Berylia vom aggressiven Nachbarstaat Crimsonia bedroht wird. Die Teilnehmer der Übung haben eigens eine fiktive digitale Infrastruktur aufgebaut, mit Wasser- und Stromversorgung, Handel, Marineschiffen. Jede teilnehmende Nation bildet ein "Blue Team", das einen bestimmten Teil von Berylia beschützt. Das "Red Team" aus Vertretern aller Länder sitzt in Tallinn und greift die "Blue Teams" permanent an. "Insofern", sagt Kammermeier, "ein sehr realistisches Szenario, das uns die Gelegenheit gibt herauszufinden, wo wir stehen."

Michael Böttcher ist bei den Berliner Wasserbetrieben für die Cybersicherheit zuständig
©Philipp von Ditfurth/stern

Am Ende der zweitägigen Übung werden die Deutschen den achten Platz belegen, also, wie in den Jahren zuvor auch, im Mittelfeld landen. "Wir stehen ganz gut da, es gibt aber bei uns wie überall im Bereich digitale Sicherheit noch großen Nachholbedarf."

Während er das sagt, wird die berylische Wasserversorgung angegriffen, bestimmte chemische Parameter übersteigen auf einmal die Grenzwerte, die Regierung empfiehlt ihrer Bevölkerung: Kauft nur noch verpacktes Wasser. Ein Horrorszenario. Und eines, das Michael Böttcher in Berlin-Friedrichshagen tagtäglich und ganz real zu verhindern versucht.

Böttcher ist ein großer Mann, der die Haare zum Pferdeschwanz gebunden hat, ein Bart rahmt seinen Mund ein. An einem Donnerstag im Mai steht er im Test- und Entwicklungslabor des Wasserwerks Friedrichshagen. Böttcher ist bei den Berliner Wasserbetrieben zuständig für die digitale Sicherheit. Er sagt: "Ein Zaun mit Stacheldraht und ein Pförtner reichen heute lange nicht mehr aus."

Die Berliner Wasserbetriebe sind der größte Wasserversorger Deutschlands und gehören damit zu den sogenannten Kritischen Infrastrukturen, im Behördensprech Kritis genannt, also jenen Anlagen, die für das Funktionieren einer Gesellschaft fundamental sind: Strom, Wasser, Internet, Notrufe etwa. Böttcher geht zu einem Computer, loggt sich ein und zeigt die Software, mit der die IT der Wasserbetriebe

permanent überwacht wird. 18 aktuelle Vorfälle zeigt das System, zwei davon kritisch. Böttchers Job ist es, die digitale Infrastruktur der Wasserbetriebe so zu gestalten, dass die Standardangriffe automatisch abgewehrt werden und die wenigen wirklich gefährlichen Angriffe erkannt und herausgefiltert werden, um sie bekämpfen zu können. Seine Strategie: das Zwiebelprinzip. "Je wichtiger das System, je relevanter die Information, desto tiefer steckt das in der Sicherheitsstruktur. Wer da ranwill, muss viele Verteidigungswälle überwinden."

Claudia Eckert (l.) erforscht die digitale Sicherheit von Unternehmen, Michael Cyl testet sie

Böttcher hat das System in den letzten zwanzig Jahren praktisch von null aufgebaut. "Als Pastorensohn glaube ich immer an das Gute im Menschen. Als Sicherheitsbeauftragter der Wasserbetriebe muss ich an das Schlechte denken. Überall mögliche Horrorszenarien, und das nicht nur bei uns, sondern bei allen Versorgern."

Inzwischen hätten er und seine Kollegen der anderen Kritis alles ganz gut unter Kontrolle. Das hänge, sagt er, ganz wesentlich mit dem IT-Sicherheitsgesetz zusammen. Vor vier Jahren wurde es vom Bundestag beschlossen, es schreibt Betreibern der großen Kritischen Infrastrukturen Mindeststandards bei der IT-Sicherheit vor. Mit dem Gesetz sei Ordnung in den Wildwuchs gekommen, sagt Böttcher. Das Problem: Kleinere Unternehmen werden davon nicht erfasst.

Risiken kaum zu überblicken

Böttcher verlässt den Raum mit den Rechnern und macht sich auf, das Wasserwerk zu besichtigen, er möchte konkret machen, worum es in seinem Job geht: das Pumpwerk, die Frischwasservorräte, die Aufbereitungsanlagen. Alles ist mit allem vernetzt, Hunderte Stellen, an denen man angreifen und die Wasserversorgung der Hauptstadt lahmlegen könnte.

Die IT-Systeme, erzählt er, würden zunehmend so komplex, dass die Risiken von einem Einzelnen kaum noch zu überblicken seien. "Eine einzige Schwachstelle in einer von Tausenden von Komponenten reicht Cyberkriminellen aus, um in ein Gesamtsystem einzudringen", sagt Böttcher. Und es gebe immer irgendwo eine Schwachstelle. "Das Problem ist also: Wenn jemand nur genug Zeit und Geld hat, kommt er überall rein." Und könnte dann die Wasserversorgung der Hauptstadt lahmlegen.

IT-SICHERHEIT

Hacker in USA stiehlt Daten von gut 100 Millionen Bankkunden

Seine Schlussfolgerung wirkt vor diesem Hintergrund logisch: Die Kronjuwelen, also die für die Versorgung der Bevölkerung unerlässlichen Teile, können im Zweifel jederzeit komplett vom Netz genommen und analog betrieben werden. "Das fühlt sich nicht sehr fortschrittlich an. Eine bessere Lösung gibt es aber nicht", sagt Böttcher. Für den Fall der Fälle haben sie hier immer bergeweise verpacktes Wasser vorrätig.

Im Zweifel analog – das ist der Goldstandard der IT-Sicherheit im Jahr 2019.

Wenn man beim Wort "Hacker" an blasse, dünne Jungs denkt, die in abgedunkelten Räumen vorm Rechner kauern, dann sieht Michael Cyl nicht aus, wie man sich einen Hacker vorstellt. Er ist ein junger Mann, nicht sehr groß, dafür sieht man ihm an, dass er viel Sport treibt. Cyl ist ein vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierter Penetrationstester, also eine Art geprüfter und bezahlter Hacker: Unternehmen beauftragen seinen Arbeitgeber Datenschutz-Cert damit, die eigene IT-Sicherheit von außen zu testen. Er war vor einigen Jahren der 14. Mitarbeiter des Unternehmens – heute sind es 150. Es gibt offensichtlich viel zu tun.

Alle Systeme haben Lücken

Wenn Cyl ein Unternehmen testet, schaut er, wie weit er kommt – und gibt dem Auftraggeber dann Empfehlungen. "Irgendeine Lücke finde ich immer", sagt Cyl.

Er sitzt in seinem Büro in Bremen, mit Blick auf die Weser. Vor ihm liegt ein Stapel Berichte. Um welche Unternehmen es geht, dürfen wir nicht schreiben. Kein Unternehmen wolle in der Zeitung stehen, weil es seine IT-Sicherheit nicht im Griff hat. Und kein einziger Bericht über ein Unternehmen nenne keine Mängel. Ein kleinerer Versorger etwa, der vom IT-Sicherheitsgesetz nicht erfasst wird, übertrug bis vor Kurzem alle Daten unverschlüsselt – bekommt ein Hacker da Zugriff, kann er alle Informationen absaugen, inklusive Zugangsdaten. Die Türen stehen ihm dann offen.

RUSSISCHER GEHEIMDIENST GEKNA...

Hacker-Angriff auf FSB enthüllt: So will der KGB-Nachfolger das Internet beherrschen

Von Malte Mansholt

"Das sind schlimme Anfängerfehler", sagt Cyl. "Gerade bei den ersten Tests finden wir so etwas praktisch immer." Dabei sei es heute gar nicht mehr so schwierig, sich zu schützen. Es koste halt Geld. "Wenn man in die entsprechende Hard- und Software investiert, ein paar Regeln befolgt und nichts am Code der Produkte ändert, ist man gut geschützt."

Inzwischen ist eine Erweiterung des IT-Sicherheitsgesetzes in der Ressortabstimmung, die Vorgaben auch für kleinere Kritis sollen härter werden, die Behörden weitreichende Befugnisse bekommen, nicht mehr nur abzuwehren, sondern selbst in Systeme einzudringen. Die Kritik an dem Gesetz ist groß, das BSI würde zu einer "Hackerbehörde", sagen Datenschützer.

Sicher ist aber: Bei den Behörden muss sich dringend etwas ändern. Wer mit der S-Bahn in den Norden von München fährt, weit raus, erst vorbei

an der Allianz-Arena und dann noch eine Weile an Feldern und Kühen, der kommt in das Zentrum der deutschen Cyberabwehr: das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit. Claudia Eckert ist Professorin und Leiterin des Instituts. Sie sitzt in ihrem Büro und sagt: "Es gibt in Deutschland unendlich viele Cyberbehörden, aber keine einheitliche Cyberdoktrin." Etwa 40 Behörden sind es auf Bundes- und Länderebene. Die digitale Verwundbarkeit der Bundesrepublik ist insofern auch eine Folge des Föderalismus.

URSACHE WIRD ERMITTELT

Twitter-Account von Scotland Yard geknackt

Dabei bräuchte Deutschland, sagt Eckert, eine Art Internetpolizei. Wirklich große Unternehmen hätten das Geld, und wirklich wichtige Kritis würden vom IT-Sicherheitsgesetz gezwungen, sich um ihre Cybersicherheit zu kümmern. Wenn aber ein Mittelständler irgendwo im Schwabenland am Samstag um 11.30 Uhr feststellt, dass jemand in sein System eingedrungen ist und Patente liest – dann hat er niemanden, den er anrufen könnte und der dann kommt, um ihm zu helfen. Außer privaten Dienstleistern. Das sei aber teuer und deswegen unbeliebt.

Zunehmend trübe Stimmung

Claudia Eckert sagt oft: "Das macht mir etwas Sorge." Zwischen den Sätzen hört man heraus, dass das eine Untertreibung ist. Im Laufe des Gesprächs verlagert Eckert ihren Blick von der Vergangenheit über den Istzustand in die Zukunft. Ihre Stimmung wird dabei, so scheint es, zunehmend trüb.

"Das Thema der nächsten Jahre wird künstliche Intelligenz sein", sagt sie. Die Idee von KI sei, dass der Algorithmus dauernd dazulernt und selbst Entscheidungen trifft. Wer KI angreifen wolle, der müsse gar nicht das System selbst angreifen. "Wenn ich die Daten manipuliere, auf deren Grundlage die KI ihre Entscheidungen trifft, funktioniert das System ja trotzdem noch korrekt. Es trifft nur die falsche Entscheidung."

Schon bald wird KI ganz wesentliche Bereiche unseres Lebens bestimmen – von der Industrie 4.0 bis zu Computern, die Menschen operieren. "Diese Systeme abwehrfähig zu machen – das ist die Aufgabe der nächsten Jahre", sagt Eckert. Eine Aufgabe, die ihr "etwas Sorge" bereite.

ERFAHREN SIE MEHR:

"DEIN KIND AUCH NICHT"

"Ich habe mich unwohl gefühlt": Wie das peinliche Shooting für Wilson Gonzalez und Toyah war

NEON

AUCH MÄNNER SIND DABEI

Mary Poppins trifft James Bond – das College für "Super-Nannys"

Nido

CYBERKRIMINALITÄT

Die Jagd auf Avalanche

ERBITTERTER KONFLIKT

Huawei trotzt den USA - und beginnt in Europa den 5G-Netzausbau

MEDIENBERICHT

Amazon lässt Alexa-Mitschnitte im Homeoffice auswerten

REAKTION AUF EU-VORWÜRFE

Google bittet Suchmaschinen zur Kasse bei Auswahl in Android

SPRECHER BESTÄTIGT

Instagram und WhatsApp bekommen Namenszusatz «von Facebook»

STREAMING

Darum will die Netflix-App plötzlich Zugriff auf Ihre Fitness-Daten

ERBITTERTER KONFLIKT

Huawei trotzt den USA - und beginnt in Europa den 5G-Netzausbau

IPHONE-GERÜCHTE

iPhone 2019: Dieses kommende Feature hatte Steve Jobs noch verspottet

Von Malte Mansholt

MARKT-ENTWICKLUNG

Die Krise des (Luxus)-Smartphones

Von Malte Mansholt

WISSENSCOMMUNITY ›

Neueste | Meist beantwortete

Wie viel Geld darf unser Sohn (15) steuerfrei über das Internet verdienen?
Unser Sohn nimmt über verschiedene Plattformen im Internet Geld ein. Zum einen sind es Werbeeinnahmen, zum anderen wird er von Firmen bezahlt wg. seiner hohen

Alle paar Minuten bricht Verbindung zum Internet weg, HILFE
Hallo, ich habe ein Repeater von Netgear, mit dem ich an meinem PC mit LAN-Kabel verbunden bin. Seit ca 3 Wochen haben wir einen neuen Router (Speedport W 925v

Suche einen Filmtitel
im Internet werden Morde gezeigt, je höher die Zuschauerquote ist, um so schneller stirbt das Opfer

Handy nass?
Gestern habe ich meine Schutzhülle gewaschen und es ist Wasser in mein Handy gekommen Jetzt geht es manschmal an geht wieder aus und ist dann schwarz Gibt es irgendein weg um es zu

Nachrichten vom 05.08.2019 | © stern.de GmbH | Die digitale Front: So wappnet sich die Bundeswehr gegen Hacker-Angriffe