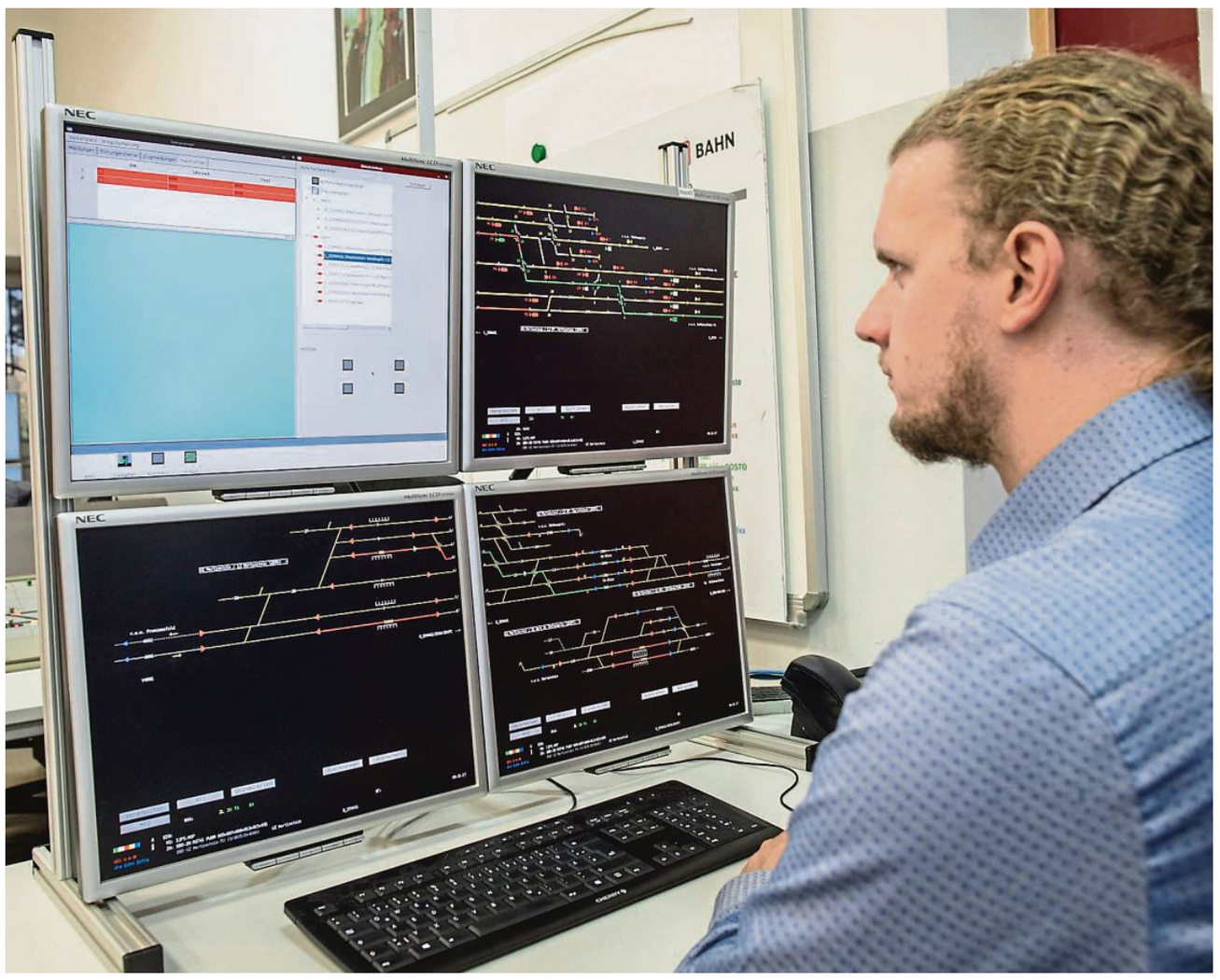
Telefon (089) 53 06-410
blickpunkt@merkur.de
Telefax: (089) 53 06-86 57

CYBERSICHERHEIT

Der Wettlauf gegen die Hacker

Hackerangriffe auf Verkehrssysteme oder Kraftwerke: Das ist für IT-Spezialisten ein Albtraum, aber auch für den Bürger eine Gefahr. Forscher wie das Garchinger Team um die TU-Professorin Claudia Eckert arbeiten daran, Angriffsziele sicherer zu machen.

VON KATHRIN BRACK



Ein Netzwerk sichern ist das Fachgebiet von Christian Schlehuber, Teamleiter Cybersecurity bei der DB Netz AG. DPA

Garching/Darmstadt – Der Angriff startete mitten im Winter und traf die Menschen unvorbereitet. Hacker attackierten mehrere Energieversorger. Mithilfe einer Schadsoftware legten sie innerhalb kurzer Zeit 30 Umspannwerke und Schaltanlagen lahm. Für fast 230 000 Menschen in der Ukraine fiel der Strom aus. Die Cyberattacke im Dezember 2015 gilt als beispiellos und ist bis heute nicht aufgeklärt. Die Angreifer führten nicht nur den Ukrainern, sondern auch dem Rest der Welt vor Augen, wie verwundbar vernetzte Systeme sind.

Forschen, damit der schlimmste Fall gar nicht erst eintritt

„Angesichts der Vernetzung sind die Wege vielfältig und das Schadenspotenzial immer gewaltig“, sagt Claudia Eckert, Lehrstuhlinhaberin für IT-Sicherheit an der TU München. Massive Attacken verhindern, den Hackern einen Schritt voraus zu sein: Das ist die Aufgabe von Wissenschaftlern wie Eckert. Sie forscht mit ihrem Team am Fraunhofer-Institut für Angewandte und Integrierte Sicherheit, kurz: Fraunhofer AISEC, in Garching (Kreis München) auf dem Gebiet der Cybersicherheit. Das AISEC, das derzeit zum Cybersicherheitszentrum ausgebaut wird, zählt zu den wichtigsten Einrichtungen für Sicherheitsforschung in Europa.

Hier entstehen Sicherheitslösungen, nicht nur, aber auch für die Unternehmen am IT-Standort München. Schon vor Jahren haben sich fast hundert Firmen und Forschungseinrichtungen im Sicherheitsnetzwerk München zusammengeschlossen. Denn neben staatlichen Netzwerken sind Wirtschaftsunternehmen begehrte Ziele für Hacker. Fachleute sprechen von kritischen Infrastrukturen, wenn sie besonders bedrohte Netze meinen. „Dazu gehören neben Energie- und Wasserversorgung auch die Verwaltung und Telekommunikation, aber auch Flughäfen und Bahnhöfe“, erklärt Eckert. „Ganze Branchen wie das Gesundheitswesen, die Ernährungsindustrie oder das Finanzwesen fallen ebenfalls darunter, und im Zuge der Digitalisierung zunehmend das produzierende Gewerbe mit vernetzten Produktionsanlagen.“

Für einen potenziellen Angriff, so Eckert, gibt es die unterschiedlichsten Szenarien. Gelingt Angreifern beispielsweise der direkte Zugriff auf Steuerungsrechner von Industrieanlagen könne der Angreifer die Anlage manipulieren, zum Stillstand bringen, dafür sorgen, dass fehlerhafte Produkte produziert werden oder die Zerstörung bewirken. „Solche Szenarien sind keineswegs unrealistisch“, sagt die Institutsleiterin. „Ersetzt man in dem Szenario die Industrieanlage durch ein Krankenhaus und die Steuerungskomponente durch ein medizinisches Gerät, beispielsweise ein Röntgengerät, kann das Angriffsmuster gleich ablaufen, aber mit völlig anderen, dramatischen Folgen. Zum Beispiel, wenn die Strahlendosis des Röntgengeräts manipuliert werden kann.“

Prof. Dr. Claudia Eckert leitet das Fraunhofer AISEC in Garching.

Für Angreifer gibt es vielfältige Wege, sich Zugang und Zugriff auf vernetzte Systeme zu verschaffen. So kann über einen USB-Stick oder über eine manipulierte Webseite Schadsoftware geladen und ausgeführt werden, die dem Angreifer Türen in das System öffnet oder vertrauliche Daten an den Angreifer sendet.

Der Schaden, den eine massive Attacke anrichten kann, kann politische Gegner ebenso anlocken wie Terroristen und andere Kriminelle, die mit Erpressung Geld machen wollen. „Es geht immer darum, was das Ziel des Angriffs ist“, sagt Eckert. Von Datendiebstahl über Spionage bis zur Kontrollübernahme, um die zivile Ordnung eines Staates zu stören, sei alles denkbar.

Trotzdem gibt es Möglichkeiten, ein Netzwerk effektiv zu schützen. Dafür braucht man einen Plan des Netzwerks, wie bei einem Gebäude. „Bildlich gesprochen muss man wissen, welche Türen wo sein müssen und wer durch welche Türen unter welchen Bedingungen gehen darf.“ Das heißt auf die IT übertragen: Man muss definieren, welche Teile des Unternehmensnetzes besonders schützenswert sind. Zudem benötigt man klare Zugriffsregeln für bestimmte Teile der IT-Infrastruktur. „So lässt sich das Risiko beherrschen“, sagt Eckert. Mit sogenannten Penetrationstests übt man den Ernstfall: Das Netzwerk wird Stresstests ausgesetzt. Man simuliert einen Angriff und versucht so, Schwachstellen zu finden und zu beseitigen. „Ein Angriff lässt sich vielleicht nicht verhindern, aber er ließe sich abwehren und der mögliche Schaden begrenzen.“

400 Kilometer von Garching entfernt arbeiten Unternehmen ebenfalls daran, denn schlimmsten Fall zu verhindern. Im hessischen Langen befindet sich eine von vier Kontrollzentralen der Deutschen Flugsicherung (DFS). Die übrigen sind am Flughafen München, in Bremen sowie bei Karlsruhe angesiedelt. Dort und im Tower an 16 Flughäfen sind die rund 2000 DFS-Lotsen im Einsatz. Täglich überwachen sie an einem komplexen Radar- und Computersystem bis zu 10 000 Flüge im deutschen Luftraum.

„Die absolute Sicherheit gibt es nie. Aber dass jemand von außen reinkommt, ist sehr unwahrscheinlich“, sagt ein DFS-Experte. Das operative System sei von der Außenwelt abgeriegelt. Über das geschlossene Netz werden Fluginformationen und Radardaten übertragen. Es sei streng getrennt vom Netz für die Bürokommunikation. In der Kontrollzentrale, deren Gebäude eine eigene Stromversorgung besitzt, gilt eine besondere digitale Schutzklasse. „Wir nennen es Schalenmodell“, sagt der Experte. Es gebe mehrere Lagen von Firewall-Ringen. „Durch die muss ein Angreifer erst mal durch, bis er an den Kern unseres operativen Geschäfts käme.“ Bislang sei erst eine Attacke registriert worden. Vergangenen Herbst habe ein Angreifer mit chinesischer Adresse versucht, einzudringen. Er scheiterte schon an der ersten Schicht.

Die Angriffe werden zunehmen, glauben die Unternehmen

An der digitalen Vernetzung führt für die Luftraumüberwacher kein Weg vorbei. Mit der analogen Punkt-zu-Punkt-Verbindung, über die die Kontrollzentren früher mit den Radaranlagen verbunden waren, ist der angestiegene Luftverkehr nicht mehr zu bewältigen. In Langen ist man sicher: „Die gezielten Hackerangriffe werden zunehmen.“

Dafür rüstet sich auch die Deutsche Bahn. Hinter dem Hauptbahnhof in Darmstadt liegt das Eisenbahnbetriebsfeld. Die Simulationsanlage stellt seit 100 Jahren den Bahnbetrieb im Kleinen dar. Zu sehen sind Bahnübergänge, Signale und vier Generationen von Stellwerksanlagen. Hier führt die Bahn Sicherheitstests durch – künftig sollen auch Cyberattacken durchgespielt werden.

Geplant ist ein großes Digitalisierungsprogramm, bei dem das Stellwerksystem vernetzt und die Zug-zu-Zug-Kommunikation ausgebaut wird. Das birgt Risiken: „Alles, was man sich vorstellen kann, ist prinzipiell möglich“, sagt Christian Schlehuber, Teamleiter Cybersecurity bei der DB Netz AG. Soll heißen: Von Verspätungen bis zum absichtlichen Herbeiführen von Unfällen rechnet die Bahn mit allem. Eine hundertprozentige Sicherheit könne es nicht geben, meint Schlehuber. Aber: „Man muss zumindest sagen können: Wir haben das getan, was möglich war.“

Mit Material der dpa

So können Sie Ihren Computer vor Angriffen schützen

Absolute Cyber-Sicherheit, das wiederholen Experten gebetsmühlenartig, kann es nicht geben. Nicht für Unternehmen und auch nicht für Privatpersonen. Allerdings kann jeder bestmöglich für die Sicherheit seiner Daten sorgen.

„Es gibt drei Dinge, die jeder tun kann und auch tun sollte“, sagt Robert Helling. Der Physiker arbeitet an der LMU München und ist Mitglied beim Chaos Computer Club München (muCCC). Der deutschlandweite CCC mit Hauptsitz in Hamburg gilt als die größte europäische Hackervereinigung und ist seit über 30 Jahren aktiv.

1. Updates ausführen
„Sagt der PC, dass ein Update zur Verfügung steht, sollte man das auf jeden Fall machen“, rät Helling. Neuere Versionen des Betriebssystems enthalten nicht nur neue oder erweiterte Funktionen, sie schließen auch Sicherheitslücken. „Sie sollten nicht aus Faulheit auf Updates verzichten.“

2. Backup erstellen
Sichern Sie regelmäßig Ihre Daten auf einer externen Festplatte. „Sollte wirklich jemand den Computer attackieren, sind zumindest die Daten gerettet.“ Und das Gerät kann in den letzten gespeicherten Zustand zurückversetzt werden. „Das funktioniert allerdings nur, wenn sich das Backup wiederherstellen lässt – das sollten Sie testen.“

3. Vorsicht bei fragwürdigen E-Mails
Jeder kennt diese E-Mails: Aufforderungen, auf Links zu klicken, Anhänge zu öffnen oder persönliche Daten einzugeben – ein potenzielles Einfallstor auf Ihren PC. „Öffnen Sie keine Anhänge, wenn Sie den Absender nicht kennen oder er Ihnen seltsam vorkommt. Und klicken Sie keine Links an“, sagt Helling. „Wenn Sie bei einem Service wie Paypal Daten aktualisieren sollen, dann machen Sie das direkt auf der Website.“ kb

Schutzschilde gegen Cyberangriffe

IT-Sicherheitsgesetz soll vor Attacken aus dem Netz schützen – Regierung unterstützt bayerische Unternehmen

München – Fast jeder Bereich des täglichen Lebens ist von informationstechnischen Systemen, von sogenannter IT, abhängig. Wenn Dienstleistungen ausfallen oder gestört sind, die zum Versorgen der Menschen und für die öffentliche Sicherheit notwendig sind, kann das drastische Folgen für die Bevölkerung haben.

In Deutschland werden zu den Betreibern solcher kritischen Infrastrukturen Organisationen und Einrichtungen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur gezählt. Die Bundesregierung geht von bis zu 2000 Betreibern aus, die für das Funktionieren kritischer Dienstleistungen erforderlich sind – und die vor schwerwiegenden Cyberattacken geschützt werden müssen.

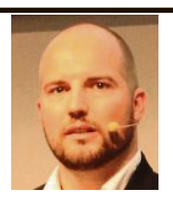
Das Bundesinnenministerium gibt jährlich einen Lagebericht zur IT-Sicherheit heraus. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kümmert sich tagesaktuell um das Thema. Für den Schutz kritischer Infrastrukturen gibt es den UP KRITIS, eine öffentlich-private Kooperation zwischen Betreibern kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen. Die Partner informieren sich über aktuelle Vorkommnisse und bewerten und schätzen Bedrohungslagen ein.

Zukunfts-Treffen: ZDB-Gründungspräsident Manfred Broy und Wirtschaftsministerin Ilse Aigner. DPA

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (kurz: IT-Sicherheitsgesetz) soll vor allem den Schutz kritischer Infrastrukturen vor Cyberangriffen verbessern. Es trat im Juli 2015 in Kraft und hat das BSI mit umfassenderen Befugnissen ausgestattet. Betreiber wichtiger Anlagen etwa aus den Bereichen Strom- und Wasserversorgung und Gesundheit werden verpflichtet, ein Mindestmaß an IT-Sicherheit einzuhalten. Und sie müssen erhebliche Störungen an das Bundesamt melden.

Für Betreiber von Webangeboten wie Online-Shops gelten erhöhte Anforderungen an den Schutz ihrer Kundendaten und der genutzten IT-Systeme. Telekommunikationsfirmen müssen unter anderem ihre Kunden warnen, wenn sie bemerken, dass deren Anschlüsse für Cyberangriffe missbraucht werden. Im Freistaat gibt es seit 2016 das Zentrum Digitalisierung Bayern (ZDB). Die Initiative der Staatsregierung mit Sitz in Garching sieht sich als Impulsgeber und Netzwerk, in dem sich Vertreter von Wirtschaft, Wissenschaft, Forschung und Politik zum Thema Digitalisierung austauschen können. Cybersicherheit spielt dabei eine wichtige Rolle. „Wir bringen Anbieter von IT-Sicherheitslösungen mit Anwendern zusammen“, erklärt die zuständige Referentin Bianca Sum. Besonders in kleinen und mittelständischen Unternehmen bestehe noch Bedarf, Lücken zu schließen. mh, kb, dpa

4 FRAGEN AN



Sascha Herzog

„Böse Hacker kennen keine Grenzen“

Sascha Herzog, 37, ist technischer Geschäftsführer der Münchner Firma Nside Attack Logic, die Cyberangriffe auf Unternehmen und Behörden simuliert, um Schwachstellen aufzudecken.

Herr Herzog, gibt es einen Unterschied zwischen guten und bösen Hackern?

Grundsätzlich gibt es drei Arten: White-Hat-Hacker untersuchen Systeme und melden Schwachstellen an die Systembetreiber oder Produkthersteller. Grey-Hat-Hacker finden Schwachstellen und veröffentlichen sie meist für jeden zugänglich. Sie halten sich nicht immer an gesetzliche Vorgaben. Black-Hats, die Bösen, wenn man so will, hacken sich illegal in IT-Systeme von Unternehmen, Privatpersonen und Regierungen. Sicherheitslücken nutzen sie, um im eigenen Auftrag oder im Auftrag von Geldgebern – oft Staaten – Systeme zu sabotieren.

Was machen Hacker?

Ein Hack ist erst einmal nichts anderes als das Umgehen einer Barriere im System. Der klassische Hacker, den Sie wohl meinen, dringt zum Beispiel in Router, Netzwerke, Webseiten, Betriebssysteme, E-Mail-Programme oder Telefone ein. Der Hacker übernimmt sie, um Daten zu stehlen, Spionage zu betreiben oder Prozesse zu sabotieren. Oder er versucht, aktuelle politische Entwicklungen zu beeinflussen.

An welchen spektakuläreren Hack erinnern Sie sich?

Besonders spektakulär war die Geschichte um den Wurm Stuxnet, der wahrscheinlich als Test von der israelischen Regierung und der NSA entwickelt wurde, um die Angreifbarkeit der Atomkraftwerke im Iran zu testen. Der Wurm konnte sich automatisch über einen USB-Stick weiterverbreiten. Die Urheber konnten die Leistung der Zentrifugen so weit runterdrehen, bis die Anreicherung von Uran nicht mehr funktionierte.

Kennen Hacker ethische Grenzen?

Die meisten Black-Hat-Hacker sicherlich nicht. Die Cybercrime-Szene hat Hacking extrem professionalisiert. Weil sich sehr viel Geld damit verdienen lässt, gibt es da keine moralischen Grenzen mehr. Sie haben keine Skrupel, sämtliche Systeme zu hacken oder mit Bestechung, physischem Einbruch und Social Engineering ihre Ziele zu erreichen. Anders in unserem Unternehmen: Was wir tun, ist legal. Aber dadurch, dass wir rechtlich abgesichert sind, gibt es eben auch Grenzen, die wir einhalten müssen. Das gleichen wir mit einer engen Zusammenarbeit mit unseren Kunden aus.

Interview: **Magdalena Höcherl**