Politik

Enter: Dunkelheit

Ampeln, Krankenhäuser, Atomkraftwerke – Angreifer aus dem Netz können ganze Städte lahmlegen. Über den Kampf gegen unsichtbare Gegner

Von Markus Balser

und Stefan Braun

Berlin/Bonn – Es war ein Tag im Herbst 2014, als ein Mann mit einem Notebook die Stadt Ettlingen unter seine Kontrolle brachte. 40000 Einwohner der Gemeinde am nördlichen Rand des Schwarzwalds ahnten nichts von der Attacke, die sich in den Netzen ihrer Stadt abspielte. Der Angreifer war äußerst präzise und hatte ein einziges Ziel: die zentrale Leitstelle der Stadtwerke. Ampeln, Banken, Fahrstühle, S-Bahn-Verkehr, Tankstellen – die gesamte Infrastruktur der Stadt hängt von diesem Knotenpunkt der Netze ab.

Nach nur drei Tagen Arbeit hatte der Hacker sein Ziel erreicht. Ein letztes Drücken auf die Enter-Taste hätte ihm gereicht und Strom, Wasser, Wärme wären in seiner Hand gewesen. Egal ob Fabriken, das Altenheim Stephanus-Stift oder das Diakonissenkrankenhaus – Ettlingen war dem Eindringling ausgeliefert. Einziges Arbeitsgerät: ein Laptop. Mögliche Folge: tote Telefone, abgeschaltete Mobilfunkmasten, ein stundenlanger Blackout.

Im beschaulichen Albtal bei Karlsruhe wurde damit der Albtraum internationaler Sicherheitsexperten wahr. Denn der Angriff in der Provinz machte nicht nur die Schwachstellen in Ettlingen klar. Er machte eindringlich auf eine bislang unterschätzte Gefahr aufmerksam. Behörden in vielen Hauptstädten dämmert, auf welche Risiken moderne Gesellschaften zusteuern. Die zunehmende Digitalisierung in allen Lebensbereichen eröffnet ganz neue Möglichkeiten der Kriminalität und Krisenszenarien in Dimensionen, die bislang für unmöglich gehalten wurden.

Sie beginnen an Laptops und PCs und nehmen ihren Lauf in Flugzeugen, an Bahnhöfen, in Fabriken und Krankenhäusern, in Stromnetzen oder Atomkraftwerken. Erpressung, Sabotage, Betrug – was schon im analogen Leben alarmierend klingt, könnte Ermittlern zufolge im digitalen Zeitalter noch bedrohlicher ausfallen. Auch weil Strafverfolger gerade zusehen müssen, wie die Verschleierungsmöglichkeiten im Internet, die Anonymisierung und Verschlüsselung, eine Strafverfolgung erschweren bis unmöglich machen.

Hacker Felix „FX“ Lindner, 38, von Resecurity Labs, einer der Top-Leute seines Metiers, hatte in Ettlingen jedenfalls leichtes Spiel. Zuerst schickte der Mann mit der Nerd-Brille E-Mails mit Schadprogrammen im Anhang an Mitarbeiter der Stadtwerke und gelangte so ins Firmennetz. Die zentrale Leitstelle war zwar extra geschützt. Doch Lindner fand heraus: Bei Updates öffnen sich kleine Schranken. Der Hacker knackte Zugänge weiterer Mitarbeiter, nutzte die Sicherheitslücke und war nach drei mal sechs Stunden Arbeit am Ziel. Stadtwerkechef Eberhard Oehler, 60, blies die Attacke aus dem Gästehaus der Stadtwerke ab – sie war ein geheim gehaltener Test. „Mir hat das Augen geöffnet“, sagt Oehler heute. „Ich war schockiert, dass es möglich ist, eine ganze Stadt mit einem Mausklick lahmzulegen.“

Dem Stadtwerke-Chef ist klar: „Im Ernstfall hätten es düstere Stunden in der Stadtgeschichte werden können.“ Die Gefahren aus dem Netz seien immens. „Die Politik realisiert das viel zu langsam.“ Seit Monaten wird Oehler in die Zentralen deutscher Stadtwerke und Krisenzentren eingeladen. In ganz Deutschland wollen Manager wissen, wie angreifbar ihre Netze sind. Den Verantwortlichen schwant: Die Risiken machen vor keinem Unternehmen, keiner Stadt, auch keinem Bürger mehr halt. Längst spielen nicht mehr nur Science-Fiction-Autoren durch, was passiert, wenn in ganzen Landstrichen nach einem langen Stromausfall Chaos ausbricht, Reisende stranden, Medikamente ohne Kühlung knapp werden, Telefone und Heizungen ausfallen, vielleicht sogar Börsenkurse abstürzen. Das Hamburgische Weltwirtschafts-Institut (HWWI) hat ausgerechnet, was allein Berlin ein Stromausfall kosten würde: etwa 23 Millionen Euro – pro Stunde.

Still, leise, unaufgeregt geht es zu in dem unscheinbaren, gar nicht mehr neuen Bürogebäude an einer Bonner Ausfallstraße. Knapp zwei Dutzend PCs stehen in seinem gut 40 Quadratmeter großen Lagezentrum. Es ist das operative Herzstück des Bundesamts für Sicherheit in der Informationstechnik, kurz BSI. An den Wänden hängen große Monitore, zwei bis drei Leute in Jeans und T-Shirt bilden die normale Schicht. Sie beobachten Tabellen und studieren Zahlenkurven. Ihre Aufgabe: Angriffe aufstöbern. Sie müssen darauf achten, dass im riesigen Datenstrom keine plötzlichen Anomalien auftreten, keine ungewöhnlich großen Datenflüsse oder überraschenden Massenbesuche auf Webseiten passieren, die auf einen Hackerangriff hinweisen könnten.

Die Behörde ist für den Bund die wichtigste Institution im Kampf gegen groß angelegte Cyber-Angriffe. Gegründet 1991 und zuletzt in immer kürzeren Abständen mit mehr Befugnissen, mehr Geld und inzwischen knapp 600 Mitarbeitern ausgestattet, soll sie einerseits das Netz des Bundes gegen alle Arten von Angriffen schützen. Monitore an der Wand zeigen deshalb unter anderem den Datenverkehr in der Hauptstadt. Zugleich dient das BSI aber auch als Anlaufstelle für große deutsche Unternehmen und Infrastrukturen, die sich angegriffen fühlen oder dergleichen fürchten müssen. Beim BSI laufen Informationen über neue Viren, Angriffsmuster und Trojaner zusammen. „Es geht um Vernetzung, um schnellstmöglichen Austausch, damit alle reagieren können, wenn was passiert“, sagt ein Mitarbeiter des Lagezentrums.

Wer hier sitzt, gehört zum sogenannten Cert, dem Computer Emergency Response Team, einer Art Alarm-Mannschaft für den digitalen Notfall. Wer sich darunter eine neue Internet-Polizei vorstellt, die im World Wide Web auf Verbrecherjagd geht, irrt gewaltig. „Wir haben kein Blaulicht auf dem Dach, wir haben keine repressive Funktion“, sagt BSI-Sprecher Matthias Gärtner, „wir sind eine zivile und präventive Behörde.“ Die Certlinge, wie sie intern genannt werden, können die Datenflüsse im Netz nur interpretieren. Aus eigener Erfahrung oder zusammen mit Kollegen aus anderen Lagezentren. Sei es im Inland, wo große Dax-Unternehmen inzwischen eigene Certs betreiben. Oder mit Pendants wie jenen in Ungarn, Frankreich oder auch Russland.

Zwar rüstet damit auch Deutschland im Kampf um die Hoheit im Netz auf. Doch während die nationalen Certs anderer Länder mal beim Militär, mal bei der Polizei, mal bei Geheimdiensten angedockt sind, versteht sich das BSI als zivile Behörde, die wie ein Schwamm von überall her Informationen über Schadprogramme, Virenangriffe, Trojanerattacken und Hackererfolge aufsaugt. „Wir sind zuallererst ein lernendes System“, heißt es in Bonn immer wieder. Sie wollen Angriffsmuster studieren und Sicherheitslücken aufspüren, um sich und andere auf nächste Angriffe vorzubereiten. Längst setzt sich die Erkenntnis durch: Verhindern lassen sich Angriffe auf Kraftwerke oder Verkehrswege immer weniger. Es geht vor allem darum, einmal eingedrungene Trojaner zu stoppen und weiteren Schaden zu verhindern.

Was im Ernstfall passieren kann, weiß man auch am Rande von München, wo wichtige Teile des Luftfahrtkonzerns Airbus mit seinen insgesamt 140 000 Mitarbeitern und 57 Milliarden Euro Umsatz sitzen. Kein anderer Konzern ist bislang so weit beim Schutz seiner Netze wie Airbus. Etwa 100 Millionen Euro habe die Airbus-Gruppe – früher EADS – in den Schutz vor Angriffen gesteckt, nationale „Cyber-Defense-Center“ aufgebaut. Das Ziel: sensible Informationen über Flugzeuge, Satelliten und Raketen zu schützen.

Sein Konzern habe schon viele Merkwürdigkeiten erlebt, räumt Bernhard Gerwert, Chef der Airbus-Tochter Defense & Space, ein. „Angebote sind schneller bei der Konkurrenz gelandet, als wir je geglaubt hätten.“ Und das dürfte noch die harmlose Version eines Angriffs sein. Mehr Schutz muss sein, wissen Airbus-Manager. Und doch stellt die Gefahr einen Konzern wie Airbus auch vor enorme Schwierigkeiten. Es sei nicht leicht, den richtigen Grad aus Schutz und Praktikabilität zu finden, sagt IT-Chef Guus Dekkers. Man könne kaum jedes Restrisiko ausschalten, ohne die Freiheiten zu sehr zu beschneiden. Nicht einzelne Unternehmen, ganze Gesellschaften müssten auf diese Fragen Antworten finden.

Dabei verschwimmen sogar die Grenzen zwischen Kriminalität und Krieg. Generalmajor Thomas Franz ist der höchste Militär der Nato, der dort für Cybersicherheit verantwortlich ist. Diese sei längst regelmäßig Thema bei den Sitzungen des Nato-Rates. Cyberangriffe könnten die Existenz ganzer Staaten bedrohen. In der Nato werden deshalb auch Angriffe nicht mehr ausgeschlossen, die in ihrer Dimension einem militärischen Angriff nahekommen, weil sie ein Land lahmlegen könnten. In einem solchen Fall könnte der Verteidigungsfall im Bündnis eintreten und militärische Reaktionen nach sich ziehen.

Nur: Selbst die Cyberexperten der Nato könnten womöglich nicht mit letzter Gewissheit sagen, wer den Angriff ausgeführt hat. Eine Reaktion würde das schwer bis unmöglich machen. Was bleibt, ist der Wunsch des Nato-Experten, dass die Staaten möglichst Ersatznetze bereithalten, um kritische Infrastrukturen wie Flughäfen oder besonders wichtige Regierungsnetze weiterbetreiben zu können.

Auch die Polizeibehörden in Deutschland haben auf die neuen technischen Herausforderungen reagiert.So sind die Landeskriminalämter genauso wie das BKA in Technik, Personal, Geld besser gerüstet. Doch selbst Profi-Ermittler fragen sich, ob sie der Gefahr überhaupt noch Herr werden können. Sie spüren, dass sie in einer kritischen Phase die Kontrolle über ganze Teile des Internets verlieren könnten. „Für Cyberangriffe muss man heutzutage kein Fachmann sein“, sagt BKA-Präsident Holger Münch. „Illegale Waren können in sogenannten Black Markets erworben werden. Dort werden Dienstleistungen und Software zur Begehung von Straftaten angeboten.“ Crime as a Service – das ist das Geschäftsmodell im Darknet.

Darknet – so nennen die Fahnder den verdeckten Teil des Netzes. „70 Prozent des Datenverkehrs sind heute gar nicht mehr kontrollierbar“, sagt ein hochrangiger Ermittler. „Wir gehen hier buchstäblich ins Dunkle.“ Die vielleicht wichtigste Ursache dafür sind sogenannte Tor-Netzwerke. Wer das Internet normal nutzt, tut das von einer klar identifizierbaren Adresse, der IP-Adresse. Wer seine Herkunft verschleiern will und einigermaßen internet-kundig ist, leitet seine Anfragen über zahlreiche verschiedene Server in unterschiedlichen Staaten um, bevor er zu seinem eigentlichen Ziel vordringt. Ergebnis, vereinfacht gesprochen: Irgendwann ist die wahre Herkunft nicht mehr erkennbar. Und Profis, die das gegen Bezahlung für Kunden erledigen, beherrschen das Prozedere längst perfekt.

Zumal die Nutzung solcher Tor-Netze nicht strafbar ist. Was für die einen schlicht dem Schutz der Privatsphäre dienen soll, ist für den anderen der Einstieg in eine Welt fast unbegrenzter krimineller Möglichkeiten. Das fängt beim Auftrag für den Diebstahl von Kreditkartendaten an und kann beim Verkauf von Maschinengewehren und Panzern enden. Deals werden per Chat ausgehandelt. Der Vertragsabschluss bleibt im Darknet diskret.

Und so wird aus den dunklen Geschäften ein Markt. Nach Erkenntnissen deutscher Sicherheitsbehörden ist besonders für gut ausgebildete, aber in der normalen Welt arbeitslose IT-Techniker in Osteuropa oder Afrika auf diese Weise ein ebenso lukrativer wie illegaler Arbeitsplatz entstanden. Ironie der Geschichte: Wer im Netz Rauschgift kauft, zahlt mehr, bekommt aber auch bessere Ware. „Schlechte Qualität kann sich niemand leisten, sonst kann das durch Kommentare wie bei Ebay sofort das ganze Geschäft gefährden“, heißt es bei den Sicherheitsbehörden bitter. Wie sie dem Herr werden könnten, können sie kaum sagen. Die größte Hoffnung hänge oft an jenem Augenblick, in dem „die digitale Welt wieder analog“

werde. Gemeint ist der Moment, an dem nach dem Geschäft im Internet ganz real Ware übergeben wird, sei es Rauschgift, eine Waffenlieferung oder ein gestohlenes Auto. Doch selbst da ranzukommen wird schwerer, weil sich bislang anders als früher keine langen Verbrecherbiografien entwickelt haben, die etwas über einen Dealer oder Schmuggler verraten könnten. So anonym die Tat, so anonym ist immer häufiger auch der Täter.

Die Bundestagsabgeordneten bekamen erst vor ein paar Tagen Post. Die Folgen eines Hacker-Angriffs auf ihre Parlaments-Infrastruktur waren so schwerwiegend, dass ein kompletter Neustart des gesamten Netzes nötig wird. Dafür bleibt es einige Tage abgeschaltet. Nach vier Tagen sei man dann wieder arbeitsfähig. Allerdings nur mit neuen Passwörtern.

Quelle: Süddeutsche Zeitung, Freitag, den 14. August 2015, Seite 6