Lazarus-Hacker hinter Angriff vermutet

Spuren führen zu Nordkoreas Cyberkriegern

Zürich Es war eine kryptische Folge von Zahlen und Buchstaben, die Cyberanalysten letzte Woche aufhorchen liess. «Wir haben starke Ähnlichkeiten im Code einer frühen Variante der Wanna-Cry-Software und in Schadsoftware der Hackergruppe ‹Lazarus› gefunden», sagt David Emm, leitender Datenforensiker bei der russischen Sicherheitsfirma Kaspersky. Damit gab es erste Hinweise auf die mögliche Täterschaft: Nordkoreas Hackerarmee.

Die berüchtigte Lazarus-Gruppe wird für eine ganze Reihe an hochkarätigen Cyberattacken verantwortlich gemacht – darunter der Einbruch im Firmennetzwerk von Sony im Jahr 2014 oder der Diebstahl von 81 Millionen US-Dollar von der Zentralbank in Bangladesh im Februar 2016. Insgesamt soll Lazarus laut einem Bericht von Kaspersky Angriffe auf Finanzinstitute und Firmen in 18 Ländern verübt haben.

Demnach unterhält die Hackergruppe eine Abteilung, «Bluenoroff» genannt, deren Ziel die Beschaffung finanzieller Mittel ist. «Das Ausmass von Lazarus' Operationen ist schockierend», heisst es im Bericht. Sie sei eine der erfolgreichsten Hackergruppen im Finanzbereich und bleibe «eine der grössten Bedrohungen für den Finanzsektor in den nächsten Jahren».

Kim Jong-un verfügt über eine veritable Cyberarmee

Kasperskys Cyberanalysten ist es im April erstmals gelungen, eine konkrete Verbindung zwischen Lazarus und Nordkorea herzustellen. Auf einem Server in Europa installierten Lazarus-Hacker eine Umgebung, in der sie verschiedene Angriffsmethoden testen konnten. Ein Zugriff auf den Server stammte von einer IP-Adresse aus dem Potonggang-guyok-Distrikt in Nordkoreas Hauptstadt Pyongyang. Dort befindet sich auch das Hauptquartier der Armeeführung. Das Regime investiert seit den Achtzigerjahren massiv in die Ausbildung von Computerwissenschaftlern und verfügt heute über eine Cyberarmee von mehreren Tausend Hackern. An Pyongyangs Eliteuniversität ausgebildet und handverlesen, arbeiten sie in den verschiedenen Abteilungen der Geheimdienstbehörde Reconnaissance General Bureau. Alleine im Bureau 121 sollen laut Überläufern 1800 Spezialisten für Cyberoperationen arbeiten.

Eine Sicherheitsfirma in Seoul sieht denn auch klare Zusammenhänge zwischen Nordkoreas Hackerangriffen, den Aktivitäten der Lazarusgruppe und der Verbreitung der Erpressersoftware Wanna Cry. «Bereits im letzten Jahr gab es Anzeichen, dass Nordkorea einen Angriff mit Erpressersoftware vorbereitet», so Simon Choi, Direktor der Anti-Virus-Software-Firma Hauri Inc.

Bislang sind es aber lediglich Indizien, die auf Lazarus als Urheber des Wanna-Cry-Angriffs hindeuten. Offen bleibt auch, ob die Lazarus-Gruppe Teil der nordkoreanischen Cyberarmee ist oder zumindest mit dem Regime zusammenarbeitet. Cyrill Brunschwiler, Direktor der Schweizer Sicherheitsfirma Compass Security, sieht eher Kleinkriminelle hinter dem Erpresser-Angriff. «Für eine staatlich gesteuerte Attacke sind die Hacker zu dilettantisch vorgegangen.»

Hannes von Wyl

Selbst die Vorzeige-Hochschule ETH hat Sicherheitslücken

Dass das Computervirus Wanna Cry in der Schweiz Spitäler und andere heikle Infrastruktur verschonte, bezeichnen Sicherheitsexperten als pures Glück

Barnaby Skinner und Simon Widmer

Zürich Die Schweiz schlitterte bei der weltweiten Attacke des Wanna-Cry-Virus nah an einer Katastrophe vorbei. Offiziell wurden nur 200 Rechner von Privaten und KMU infiziert; doch es hätte Tausende treffen können. Das zeigt eine Analyse offener Schweizer IP-Adressen. Sie sind so etwas wie die Identitätskarten jedes Rechners im Internet. Viele hiesige Server und Computer sind mit veralteter Windows-Software im Internet unterwegs und so ein Ziel des Wanna-Cry-Virus.

Die Zürcher Firma Binary Edge durchstöbert regelmässig das gesamte Internet nach ungeschützten Computern und filtert Schweizer Adressen heraus. Die Firma zählt 3621 Schweizer Geräte, die vom Virus Wanna Cry hätten befallen werden können, weil ihre Software veraltet ist. Das Unternehmen hat sich auch angeschaut, wo die löchrigen Systeme stehen: in Arztpraxen, bei Kantonsbehörden oder in Schweizer Hochschulen.

Zwei Rechner gehören der ETH Zürich, eine weitere der Universität Lausanne. Bei der ETH betrafen die Löcher das Institut für Raum- und Landschaftsentwicklung und das Institute for Dynamic Systems and Control; Letzteres arbeitet unter anderem an Robotern. «Alles spitzentechnologische Weiterentwicklungen», wie es auf der Instituts-Website heisst.

Auf Anfrage gab die ETH an, das Sicherheitsloch in einem Fall schon vor dem Wanna-Cry-Angriff gestopft zu haben. Das zweite Loch sei der Hochschule neu, doch auch das habe man inzwischen geschlossen.

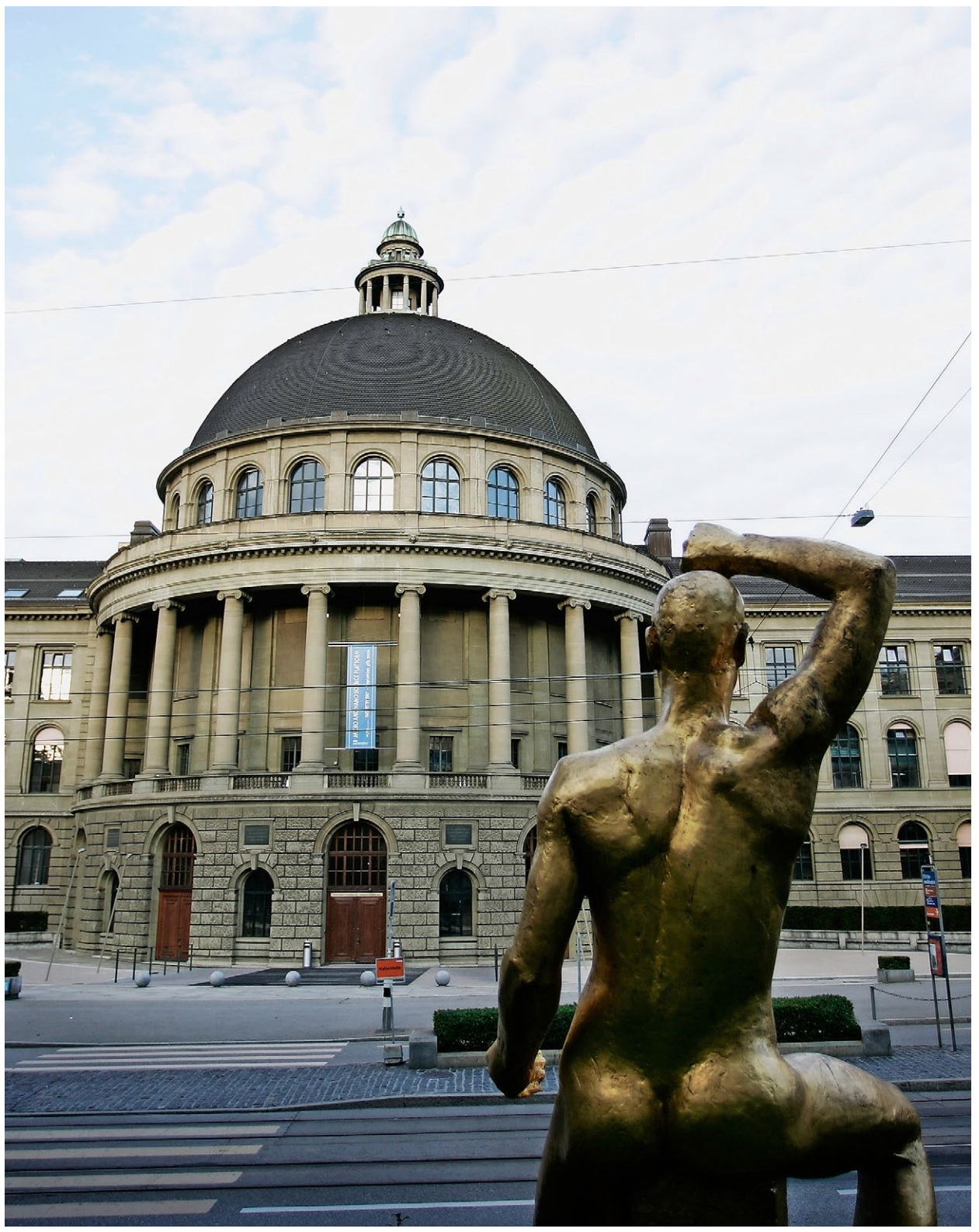
Ein Arzt öffnete infizierte Mail, die als Gerichtsschreiben getarnt war

Die ETH-Medienstelle erklärt, die Systeme mit wichtigen Finanz-, Personal- oder Studierendendaten seien trotz diesem Loch immer sicher gewesen. «Es bestand zu keiner Zeit eine Gefährdung dieser Systeme durch die Wanna-Cry-Attacke», so die Hochschule. Auch die Universität Lausanne gibt an, ihre Sicherheitslücke mittlerweile geschlossen zu haben.

Für Tiago Henriques, CEO von Binary Edge, ist der Fall allerdings klar: «Dass die Schweiz von Wanna Cry bislang weitgehend verschont wurde, hat weniger mit guten Sicherheitsstandards zu tun als mit Glück.» Henriques begrüsst, dass nach dem Wanna-Cry-Angriff viele geschädigte Firmen und Organisationen über die Gefahren im Netz zu reden beginnen. Auch in der Schweiz.

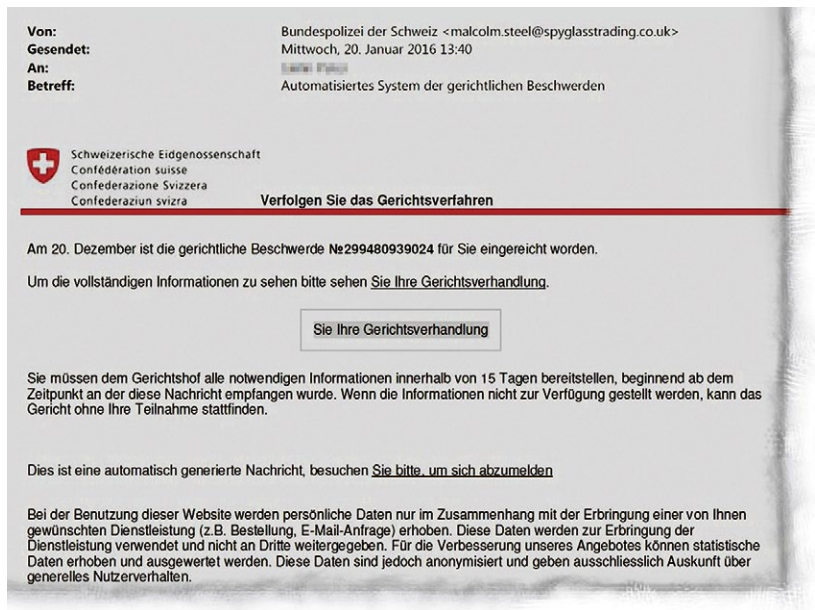
Bisher haben etwa hiesige Spitäler die sogenannten Ransomware-Attacken totgeschwiegen. Das sind Cyber-Angriffe, bei denen Angreifer Dokumente verschlüsseln und erst gegen Lösegeld wieder entschlüsseln. 44 Spitäler machten bei einer aktuellen Umfrage der SonntagsZeitung zu solchen Attacken mit. Über ein Drittel gab an, bereits Opfer eines Angriffs gewesen zu sein.

Ein Fall betrifft das Spital in der Zürcher Seegemeinde Männedorf. Im Januar 2016 erhielt ein Arzt eine Mail mit Informationen zu einer Gerichtsverhandlung. Er klickte auf den Link, die schädliche Software infizierte zehn Computer und einen Netzwerk-Server. Das Virus verschlüsselte sämtliche Daten der Computer. Auf dem Bildschirm erschien die Aufforderung, 500 Franken per Bitcoin zu bezahlen. Das Spital ging nicht auf den Erpressungsversuch ein. Mit einem Daten-Back-up konnten die Computer auf einen virusfreien Zustand zurückgestellt werden.



ETH Zürich: In zwei Instituten waren Rechner gefährdet

Foto: Justin Hession/Keystone



Von: Bundespolizei der Schweiz <malcolm.steel@spyglasstrading.co.uk>
Gesendet: Mittwoch, 20. Januar 2016 13:40
An: [redacted]
Betreff: Automatisiertes System der gerichtlichen Beschwerden

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verfolgen Sie das Gerichtsverfahren

Am 20. Dezember ist die gerichtliche Beschwerde **№299480939024** für Sie eingereicht worden.

Um die vollständigen Informationen zu sehen bitte sehen Sie Ihre Gerichtsverhandlung.

Sie Ihre Gerichtsverhandlung

Sie müssen dem Gerichtshof alle notwendigen Informationen innerhalb von 15 Tagen bereitstellen, beginnend ab dem Zeitpunkt an der diese Nachricht empfangen wurde. Wenn die Informationen nicht zur Verfügung gestellt werden, kann das Gericht ohne Ihre Teilnahme stattfinden.

Dies ist eine automatisch generierte Nachricht, besuchen Sie bitte, um sich abzumelden

Bei der Benutzung dieser Website werden persönliche Daten nur im Zusammenhang mit der Erbringung einer von Ihnen gewünschten Dienstleistung (z.B. Bestellung, E-Mail-Anfrage) erhoben. Diese Daten werden zur Erbringung der Dienstleistung verwendet und nicht an Dritte weitergegeben. Für die Verbesserung unseres Angebotes können statistische Daten erhoben und ausgewertet werden. Diese Daten sind jedoch anonymisiert und geben ausschliesslich Auskunft über generelles Nutzerverhalten.

Gefälschte Gerichts-E-Mail: Beim Anklicken des Links wurde das Virus aktiviert

Medizinaltechnologie hinkt bei IT-Sicherheit hinterher

Auch das Spital Wallis wurde angegriffen. Ende 2014 hatte ein Mitarbeiter in Sitten ein Word-Dokument geöffnet. Wie in Männedorf enthielt dieses Ransomware. Und auch hier konnte das Problem offenbar mit einem Back-up gelöst werden. Mit einem «blauen Auge» sei man davongekommen, sagt Patrick Bizeau, Informatikchef am Spital Wallis.

Bizeau ortet bei Spitälern ein grundsätzliches Problem: «Im Vergleich zu Telecomfirmen oder Banken ist die Medizinaltechnologie bezüglich Cyber-Sicherheit um zehn bis fünfzehn Jahre im Rückstand», sagt er. Teure Geräte wie ein Magnetresonanztomograf haben eine Lebensdauer von zehn Jahren, die von den Herstellern darauf installierten Betriebssysteme aber nur eine solche von fünf bis sechs Jahren. Upgrades sind oft nicht möglich. «Das ist fahrlässig», sagt Bizeau.

Das Spital Wallis will die Hersteller in Zukunft in die Pflicht nehmen. Zusammen mit anderen Westschweizer Spitälern hat es einen Katalog mit Sicherheitskriterien entwickelt, an die sich Hersteller bei Ausschreibungen zwingend halten müssen.

Wanna Cry könnte für die Schweiz also ein Weckruf gewesen sein. Philipp Zihler vom Beratungsunternehmen B-Secure aus Emmenbrücke LU sagt: «Die Hacker-Angriffe sind in den letzten Jahren raffinierter geworden. Immer öfter sind E-Mail-Angriffe von echten Nachrichten kaum zu unterscheiden.» Zihler kommt wie der Sicherheitsexperte Tiago Henriques zum Schluss: «Dass die Schweiz vom Wanna-Cry-Virus verschont geblieben ist, war reines Glück.»

Ähnlich gelagerte künftige Angriffe könnten laut Zihler hierzulande viel verheerendere Folgen haben. Wie das Grossbritannien mit Wanna Cry eben erlebt hat. Auf der Insel wurden wegen des Super-Virus Kliniken und andere Gesundheitseinrichtungen lahmgelegt, Dutzende heikle Operationen mussten verschoben werden, weil Patientendokumente blockiert waren.

Kommentar — 16, Wirtschaft — 32/33