HEUTE
16.5.2017

Der Blattmacher empfiehlt

Andreas Schaffner

Man kennt ihn als Mann mit der Fliege: **Claude Longchamp**, der umtriebige Politologe. Am kommenden Sonntag wird er **das letzte Mal vor die Kamera** treten und der Schweiz die Abstimmungsergebnisse erklären. Danach ist Schluss. Seine Firma hat er verkauft. Sicher ist: Longchamp zieht es in die Ferne, dann kommt ein Buch. Mein Kollege Max Dohner hat sich mit Longchamp getroffen und mit ihm **auf die vergangenen Jahre zurückgeblick**t. Auf schicksalhafte Jahre für die Schweiz, aber auch auf schicksalhafte Jahre für den Politologen.

Frage des Tages

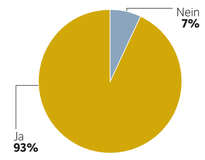
Sollen Ambulanzen nachts nur mit Blaulicht ohne Martinshorn fahren?

Ja **Nein**

Stimmen Sie online ab unter
www.aargauerzeitung.ch
www.bzbasel.ch
www.basellandschaftliche.ch
www.solothurnerzeitung.ch
www.grenchnertagblatt.ch
www.limmattalerzeitung.ch
www.oltnertagblatt.ch
«Die Umfrage finden Sie online über die Such-Funktion mit dem Stichwort «Tagesfrage»
Das Ergebnis erscheint in der nächsten Ausgabe.

Ergebnis letzte Tagesfrage

Wir haben gefragt: Führen Sie regelmässig Software-Updates durch?



Video des Tages

www.aargauerzeitung.ch/mediathek/videos

Gute Tat: Gefangen auf achtspuriger Strasse – Polizist greift durch.

REZEPT DES TAGES

Präsentiert von Annemarie Wildeisen

Gefüllte Teigwarenmuscheln mit Krautstielen

Zutaten für 4 Personen

Sauce:
1 Zwiebel mittelgross
2 Knoblauchzehen
2 Esslöffel Olivenöl
2 Esslöffel Tomatenpüree
2 dl Gemüsebouillon
400 g Dosentomaten gehackt
Salz, Pfeffer aus der Mühle

Teigwaren:
500 g Krautstiele mit schönem Grün
Salz
20 Teigwarenmuscheln
1 Zwiebel mittelgross
1 Bund Petersilie glattblättrig
1 Esslöffel Butter
125 g Doppelrahmfrischkäse mit Pfeffer
75 g Magerquark
Pfeffer aus der Mühle
50 g Parmesan gerieben
Butterflöckchen zum Überbacken

www.wildeisen.ch/suche/rezepte

Die globale Cyberattacke auf die Spitäler

«WannaCry» wird in der Schweiz in Schach gehalten

Auch in der Schweiz wurden Spitäler erpresst

In der Vergangenheit wurden Schweizer Kliniken von Hackern attackiert – und zahlten sogar schon Lösegeld. Das Gesundheitswesen ist ein Einfallstor für Cyberattacken.

VON SVEN ALTERMATT

Es ist ein ziemlich übler Schädling, der sich in britischen Spitälern ausgebreitet hat. Sein Name: «WannaCry». Doch statt auf die Gesundheit der Patienten hat er es auf die Computer in den Kliniken abgesehen. Der Schädling ist verantwortlich für einen Grossangriff, der seit Freitag weltweit ein nie da gewesenes Ausmass erreicht hat.

Hunderttausende Computer wurden von «WannaCry» infiziert. Die Ransomware hat sich auf den Rechnern installiert und Dateien verschlüsselt – mit dem Hinweis, dass diese erst gegen Bezahlung von Lösegeld wieder freigegeben werden. Das Programm ist so konstruiert, dass es möglichst viele Computer infizieren kann. Es hat demnach viel Zufall mitgespielt, dass in Grossbritannien ausgerechnet Spitäler übermässig davon betroffen waren. Die bisher unbekannten Hacker trafen 61 Zentren des britischen Gesundheitsversorgers NHS. Mediziner kamen nicht mehr an Patientenakten, Operationen und Untersuchungen mussten verschoben werden.

Die Schweizer Kliniken blieben von «WannaCry» verschont. Niemand lag auf dem Spitalbett und wurde damit konfrontiert, dass seine dringend notwendige Herzoperation verschoben wird. Dennoch gilt das Risiko entsprechender Attacken auch hierzulande als hoch. Eine Studie des ETH-Elektroingenieurs Martin Darms aus dem Jahr 2015 macht deutlich, wie anfällig besonders die internen Netzwerke von Spitälern sind. In jedem System gebe es «durchschnittlich eine kritische Stelle», so sein Befund (Ausgabe von gestern). Gewisse Spitäler schützen ihre Systeme nur mit Standard-Passwörtern.

Spitäler geben wenig preis

Für Cyberattacken besteht in der Schweiz nach wie vor keine Meldepflicht. Gefragt nach entsprechenden Erfahrungen, reagieren Spitäler bisweilen nervös. Manche wollen sich in diesem Zusammenhang gar nicht zitieren lassen, andere antworten nur summarisch. «Zu unserer Informatik äussern wir uns nicht», lässt eine angefragte Klinik gar ausrichten.

Ralph Jordi vom Informatikdienstleister Hint AG spricht von einer «Kultur des Schweigens». Die Kommunikation vieler Spitäler sei allzu defensiv, sagt er. «Cyberattacken halten sich nicht an Landesgrenzen, auch die Schweiz ist betroffen. Aus Angst vor Imageschaden will darüber aber kaum jemand öffentlich reden.» Dabei sei genau das Schweigen mitunter verantwortlich dafür, dass sich viele des Problems nicht bewusst sind. Ein Teufelskreis.

Die Hint AG mit Sitz im aargauischen Lenzburg arbeitet für 15 Spitäler, zu ihrem Angebot gehört der Schutz vor Cybercrime. Noch vor einem Jahr sei eine betreute Klinik durchschnittlich einmal pro Monat von Hackern angegriffen worden, so Jordi. Heute würden bis zu drei Attacken pro Monat registriert. Die Behörden warnen grundsätzlich davor, Geld an Hacker zu überweisen. Es gebe keine Garantie, dass Daten danach wieder entschlüsselt werden. Dennoch kommt es immer wieder zu Lösegeldzahlungen, weil Betroffene keinen anderen Ausweg sehen.

Laut einer Studie der Softwarefirma Symantec sind weltweit 34 Prozent der Firmen bereit, den Forderungen von Hackern nachzukommen. Der «Nordwestschweiz» sind zwei Fälle bekannt, in denen Schweizer Kliniken nach Hackerattacken mehrere hundert Franken Lösegeld bezahlten.

Es geht um Leben und Tod

Die Bedrohung hat eine neue Dimension erreicht, seit das Internet nicht nur Computer verbindet, sondern Autos, Maschinen oder Haushaltsapparate. Auch in Spitälern sind viele Geräte ans Netz angeschlossen. Narkosegeräte oder Spritzenpumpen sind längst online. Plötzlich geht es bei einem Hackerangriff um Leben und Tod. «Die Täter wissen, dass ein Spital schnell reagieren und seine Informatikinfrastruktur zur Verfügung haben muss», heisst es bei der Meldestelle für Internetsicherheit (Melani) des Bundes.

Das Gesundheitswesen steckt in der Klemme. Die Digitalisierung schreitet voran, die Effizienz steigt. Es ist kaum mehr denkbar, dass Daten und Systeme nicht vernetzt sind. Hackern öffnen sich damit immer mehr Einfallstore für Attacken. Gleichzeitig warnen Fachleute, dass die Branche bei der Cybersicherheit um Jahre hinterherhinkt. Oder wie es Sicherheitsexperte Darms ausdrückt: «Mit ein wenig Fachwissen und den richtigen Tools aus dem Internet ist es möglich, einen beträchtlichen, sogar lebensgefährlichen Schaden anzurichten.» Das Schutzniveau in den Kliniken unterscheide sich stark.

Ständig kommen zudem neue Risiken hinzu. Unterdessen gibt es Schadprogramme, die auf infizierten Websites ganz ohne Anklicken heruntergeladen werden. Immerhin sei das Bewusstsein für Cyberattacken in den Spitälern gestiegen, sagt Ralph Jordi. «Vielerorts wird heute in die Sicherheit investiert.»

Anfällige Betriebssysteme

Gerade medizinische Geräte wie Tomografen oder radiologische Apparate sind anfällig. Obwohl sie nicht selten mit dem alten Betriebssystem Windows XP laufen, sind sie eng ins Informatiknetz der Spitäler eingebunden. Jordi weiss: Updates werden teilweise nicht durchgeführt, weil sie die Zulassung gefährden.

Eine fatale Schwachstelle. In britischen Spitälern ist das Problem nicht erst seit «WannaCry» bekannt. Bereits im vergangenen Januar wurde publik, dass ihre Computer schon vor Jahren ins Visier von Hackern geraten sind. Dutzende Spitäler überwiesen bereits einmal Geld, um die Herrschaft über die Rechner wieder zurückzubekommen. Die Warnzeichen verpufften offenbar.

CYBER-KRIMINALITÄT

Nur vorsichtige Entwarnung

Nach der globalen Cyberattacke war gestern die Angst vor einer zweiten Angriffswelle gross. Doch die europäische Polizeibehörde Europol hat eine vorsichtige Entwarnung gegeben. Die Schweiz kam wohl mit einem blauen Auge davon. Experten und Behörden waren davon ausgegangen, dass die Zahl der infizierten Computer steigt, weil am Montag zahlreiche Computer erstmals nach dem Wochenende wieder hochgefahren wurden.

Grosse Schweizer Firmen waren nach eigenen Angaben nicht unter den Opfern des Cyber-Angriffs, fuhren aber als Reaktion ihr Sicherheitspositiv hoch. Der Spitalverband H+ hatte auf Anfrage keine Kenntnis von betroffenen Spitälern oder Kliniken. Gleiches teilten Swisscom, SBB, Migros, UBS und Credit Suisse sowie Novartis mit.

In Frankreich stand am Montag in einem der grössten Werke des Autoherstellers Renault im nordfranzösischen Douai die Produktion noch still. Informatiker sollten verhindern, dass sich das Virus von möglicherweise infizierten Rechnern aus weiter verbreite. 3500 Mitarbeiter blieben zu Hause.

Auch in Asien blieb die für den Montag befürchtete Welle von Computerstörungen aus. Zwar wurden Störungen gemeldet, massive Ausfälle von Computernetzen gab es zunächst aber nicht. In China waren es 30 000 Opfer – rund 200 000 Computer wurden dort attackiert. Mehr als 20 000 Tankstellen des chinesischen Öl-Giganten CNPC gingen demnach offline; Kunden konnten nur noch mit Bargeld zahlen. In Japan meldete der Technologiekonzern Hitachi IT-Probleme. In der indonesischen Hauptstadt Jakarta waren zwei Spitäler betroffen. (SDA)

«WannaCry» hat in Grossbritannien das Gesundheitssystem lahmgelegt. In der Schweiz kam es nicht dazu. GETTY IMAGES

Spitäler aus der Region geben Entwarnung

Aargau Baden musste schon Cyberattacken abwehren

Die Kantonsspitäler im Aargau waren von der «WannaCry»-Attacke nicht betroffen. Man ist sich der Risiken aber durchaus bewusst. «Heute kann sich kein Unternehmen und keine Institution mehr vor solchen Angriffen sicher fühlen. Die Gefahr besteht immer, überall und für jeden», sagt Andrea Rüegg, Sprecherin des Kantonsspitals Aarau. Dass man schon einmal von einer Attacke betroffen war, will Rüegg nicht bestätigen. Es sei nicht im Interesse des KSA, diese Thematik in der Öffentlichkeit «auszuschlachten». Seit dem 1. Januar 2016 werden sämtliche IT-Belange des Spitals Zofingen durch die Informatikabteilung des Kantonsspitals Aarau abgedeckt.
Erfahrungen mit Cyberattacken hat das Kantonsspital Baden (KSB) bereits machen müssen. «Angriffe auf die Infrastruktur des KSB hat es schon gegeben», sagt Sprecher Stefan Wey. Diese hätten erfolgreich abgewehrt werden können. Lösegeldforderungen seien bislang keine eingegangen. Viele Bedrohungen hätten schon früh abgeblockt werden können, andere seien ins interne Netzwerk gelangt. Häufigste Schwachstellen: privater Gebrauch von Webmail-Accounts und mobile Geräte. Wey: «Um den Schaden einer Infektion durch Malware möglichst klein zu halten, wird das interne Netzwerk in verschiedene Zonen und Bereiche unterteilt.» Kurzfristige Massnahmen erlassen beide Kantonsspitäler nicht. Die Lage werde permanent beobachtet. (NCH)

Basel «Wir sind der Meinung, dass wir gut geschützt sind»

Die beiden grössten Spitäler der Region Basel, das Universitätsspital Basel (USB) und das Kantonsspital Baselland (KSBL), wurden von den jüngsten Hacker-Attacken nicht getroffen. «Unsere Systeme sind auf dem aktuell notwendigen Sicherheitslevel gepatched», sagt USB-Sprecher Martin Jordan. Aus dem KSBL heisst es, man sei gegen diese Art von Angriffen seit Frühling 2016 «speziell geschützt». Beide Spitäler bestätigen aber, in der Vergangenheit von Cyber-Kriminellen attackiert worden zu sein. Bis vor Jahresfrist sei es «vereinzelt» zu Angriffen gekommen, bei denen allerdings «nur einzelne User» betroffen gewesen seien, teilt das KSBL mit. Und beim Basler Unispital spricht man von «punktuellen Infektionen», die rasch aufgespürt und eliminiert worden seien. Sowohl Unispital Basel als auch Kantonsspital Baselland sind der Ansicht, dass ihre IT genügend geschützt sei. «Wir haben alle verfügbaren Schutzmechanismen umgesetzt und sind auf dem neuesten Stand», schreibt das KSBL. Allerdings ist sich das Kantonsspital bewusst, dass die Cyber-Kriminalität immer einen Schritt voraus sei. Man beobachte die Situation laufend. Auch beim Unispital Basel nimmt man das Thema IT-Sicherheit «sehr ernst». «Wir sind der Meinung, dass wir gut geschützt sind.» So überprüfe und erweitere das Spital stets seine Sicherheitssysteme. Auch werde das Personal geschult, um es für derartige Gefahren zu sensibilisieren, betont USB-Sprecher Jordan. (BOS/HAJ)

Solothurn Regelmässige Risikoanalysen

Die Spitäler im Kanton Solothurn sind nach eigenen Angaben bisher nicht Opfer von Hacker-Attacken geworden. Wären sie ausreichend geschützt, um sie abzuwehren? Die Solothurner Spitäler AG (soH) verfüge über eine Informationssicherheitsstrategie mit klaren Leitlinien, Verfahren und Regelungen, um sich bestmöglich vor Cyber-Angriffen zu schützen, erklärt Sprecher Oliver Schneider. Man achte «sehr pedantisch» auf die Einhaltung der vorgegebenen Sicherheitsnormen und orientiere sich dabei an internationalen Standards.
Details zum Sicherheitsdispositiv gibt man bei den Solothurner Spitälern freilich nicht preis – «grundsätzlich, aus Sicherheitsgründen». So viel sagt Oliver Schneider: Es gehören sowohl technische Massnahmen als auch klare Regelungen und organisatorische Massnahmen dazu. Zum Beispiel würden die Mitarbeitenden durch Schulungen und proaktive Kommunikation auf allen zur Verfügung stehenden Informationskanälen für die Problematik sensibilisiert und auf die möglichen Gefahren und Verhaltensmassnahmen hingewiesen. In der Solothurner Spitäler AG, zu der das Bürgerspital in Solothurn, das Kantonsspital Olten, das Spital Dornach und die psychiatrischen Dienste gehören, werden regelmässig Risikoanalysen und Assessments mit Sicherheitsexperten durchgeführt. Im Fall einer Sicherheitslücke ergreife man jeweils umgehend entsprechende Massnahmen. (MOU)

Zürich Dank regelmässigen Updates auf der sicheren Seite

Die Schadsoftware «WannaCry» hat gestern auch die Informatik-Abteilungen im Kanton Zürich beschäftigt. Kein Wunder, denn die betroffenen Windows-Betriebssysteme sind auch in der Verwaltung weit verbreitet. Doch die Verantwortlichen in den Spitälern geben gegenüber der «Nordwestschweiz» Entwarnung. Eine Sprecherin des Universitätsspitals Zürich sagt etwa, dass man vom aktuellen Angriff des Erpressungstrojaners nicht betroffen sei.
Auch in der Vergangenheit sei ihr kein Angriff in vergleichbarer Art bekannt, sagt sie weiter. Ähnlich tönt es auch von Thomas Brack, Spitaldirektor des Spitals Limmattal. Es sei in den vergangenen Tagen kein Cyberangriff registriert worden, gibt er zu Protokoll. Die Infrastruktur ist hier ausgelagert, die Lücke wurde von den Spezialisten bereits geschlossen, und es wurden regelmässige Updates vorgenommen. Deshalb sei es in der Vergangenheit auch nicht zu einem erpresserischem Ereignis gekommen.
Die Schadsoftware mit dem Namen «WannaCry» hatte sich über das Wochenende auf mehr als 200 000 Ziele in über 150 Ländern verbreitet. Besonders betroffen von der Attacke sind Spitäler in Grossbritannien. In rund einem Fünftel der Institutionen des nationalen Gesundheitsdienstes NHS war der Betrieb seit Freitagabend behindert. Mediziner kamen nicht mehr an Patientenakten, Operationen und Untersuchungen mussten verschoben werden. (NCH)

Wie die Erpresser vorgegangen sind

Geht die Attacke weiter? Was können Betroffene tun? Die wichtigsten Antworten zur Cyberattacke

VON RAFFAEL SCHUPPISSER

1 Wie kam es zum Angriff?
Cyberkriminelle haben eine Schadsoftware namens «WannaCry» in Umlauf gebracht, die auf Festplatten gespeicherte Daten verschlüsselt. Das können Dokumente oder Fotos von Privatnutzern sein, aber auch Patientendaten in Spitälern. Die Kriminellen fordern ein Lösegeld für die Daten und versprechen, die Festplatte wieder zu entschlüsseln, wenn ihren Forderungen nachgekommen wird.

2 Sind solche Erpressungen neu?
Nein, Ransomware, wie man die Erpressungstrojaner nennt, haben sich in den letzten Jahren zunehmend verbreitet. «Der Unterschied zu bisherigen Angriffen ist aber, dass sich die Schadsoftware selbstständig übers Internet als Wurm verbreitet», erklärt Candid Wüest von der IT-Sicherheitsfirma Symantec. Die Angreifer haben dafür eine Sicherheitslücke im Betriebssystem Windows ausgenutzt. Sofern die Software nicht auf dem neusten Stand und der Computer mit dem Netz verbunden ist, kann der Trojaner auf dem eigenen Rechner aktiv werden. Dafür ist es nicht einmal nötig, dass der Nutzer eine dubiose E-Mail öffnet.

3 Konnte die Attacke inzwischen gestoppt werden?
Einem jungen IT-Sicherheitsforscher gelang es am Sonntag, die Verbreitung des Computerwurms vorerst zu unterbinden. Er fand heraus, dass im Schadcode eine Art Notfallschalter eingebaut ist. Sobald ein Rechner infiziert worden ist, versucht er, Kontakt zu einer noch nicht registrierten Website aufzunehmen. Gelingt dies nicht, startet die Schadsoftware. Der Forscher liess die Website registrieren, was zur Folge hatte, dass die Schadsoftware nicht mehr aktiviert wurde. Gemäss Thomas Uhlemann von der IT-Sicherheitsfirma ESET «sind nun aber bereits Varianten der Malware im Umsatz, denen der Killswitch fehlt».

4 Geht die Attacke also doch weiter?
Einige Experten fürchten, dass es nun zu einer zweiten Angriffswelle kommen wird (ohne Killswitch). Bis zu Redaktionsschluss blieb diese aber aus. Die Windows-Nutzer dürften ihre Systeme in Zwischenzeit upgedatet haben – auch jene, die noch das veraltete Windows XP verwendeten. Für dieses hat Microsoft nämlich den Support eigentlich schon letztes Jahr eingestellt, nun übers Wochenende aber zügig reagiert und einen Patch entwickelt.

5 Alles gut also?
Gut möglich, dass «WannaCry» keinen grösseren Schaden mehr anrichten wird. Doch weitere Angriffe mit Erpressungstrojanern werden mit Sicherheit folgen. «Für Hacker ist das eine Möglichkeit, aus ihren Angriffen rasch Profit zu machen», sagt Marc Ruef von der Sicherheitsfirma Scip. Dass weitere Angriffswellen, die, nach diesem Muster aufgebaut sind, folgen werden, davon gehen Ruef aus.

6 Wie viel Geld konnten die Angreifer erbeuten?
Bis Redaktionsschluss wurden 55 000 Dollar in der digitalen Währung Bitcoin eingezahlt. Die Erpresser forderten jeweils 300 Dollar Lösegeld. Bei 200 000 infizierten Rechnern, ist das eher eine magere Ausbeute. Das Geld ist noch immer auf anonymen Bitcoin-Konten geparkt. «Das ist untypisch», sagt Candid Wüest von Symantec. Normalerweise werde das erbeutete Geld von den Hackern über Online-Casinos gewaschen, sodass der Geldfluss nicht mehr nachverfolgt werden kann. Sofern die Angreifer keine Fehler gemacht haben und stets Anonymisierungstools verwendet haben, sei es fast unmöglich, sie aufgrund von digitalen Spuren zu identifizieren.

7 Wie konnten die Angreifer die Schadsoftware programmieren?
«Die Malware basiert auf einer Sicherheitslücke der NSA», sagt IT-Sicherheitsexperte Marc Ruef. Geheimdienste klappern Betriebssysteme nach solchen Lücken ab oder kaufen die entsprechende Software auf dem Schwarzmarkt ein, um etwa in Computersysteme von Terroristen einzudringen. Vor einem Monat hat die Gruppe «The Shadow Brokers» die Sicherheitslücke publik gemacht, Ob das anonyme Kollektiv die wertvolle Information selber bei der NSA erbeutet hat oder über einen Informanten in den Besitz gekommen ist, das ist unklar. Bereits zuvor hat Microsoft die Sicherheitslücke gestopft. Zu vermuten ist, dass der Konzern informiert worden ist, dass die Lücke existiert und bald im Internet auftauchen wird. Allerdings wurde bis zu diesem Wochenende kein Update für das veraltete Programm Windows XP geschrieben.

8 Wie können Nutzer sich schützen?
Erstens sollen regelmässig Back-ups erstellt werden: Dafür eignet sich eine externe Festplatte, die nach dem Überschreiben der Daten wieder vom Netz getrennt wird; oder eine verschlüsselte Cloud wie etwa Dropbox. Zweitens soll die Software stets auf dem neusten Stand sein und es sollten keine veralteten Systeme verwendet werden, für die es keine Updates mehr gibt. Drittens: Sollen E-Mails von dubiosen Absendern nicht geöffnet werden. Viertens: Soll kein Lösegeld bezahlt werden, wenn es einen doch erwischt hat: Denn einerseits ist unklar, ob die Daten wirklich wieder hergestellt werden; andererseits wird Ransomware mit jeder erfolgreichen Erpressung bei Hackern populärer.

Plötzlich keinen Zugang mehr zu seinen persönlichen Daten.