Wochenkommentar 20/2017 von Matthias Zehnder

Die Computer sind nicht das Problem

Die Aufregung diese Woche war gross: Ein Virus namens WannaCry griff Computer auf der ganzen Welt an. Etwa 300'000 Systeme in 150 Ländern waren betroffen. In England mussten Spitäler Patienten abweisen. In Deutschland fielen Anzeigetafeln der Deutschen Bahn aus. Allenthalben hoben Experten den Zeigefinger und warnten vor Cyberterror, vor Technik-Abhängigkeit, vor der Computerzukunft. Doch das Problem liegt ganz woanders. Überzeugen Sie sich selbst.

Europol erklärte: *Das ist der grösste Cyberangriff bisher.*[1] Die Rede ist von einem Computervirus namens *WannaCry.* Auf Deutsch heisst das: *Ich könnte heulen.* Und so war es wohl vielen Besitzern von infizierten Computern in der Tat zumute. Das Virus verschlüsselte nämlich die Festplatte der befallenen Computer, so dass die Besitzer keinen Zugang mehr zu ihren Daten hatten. Es sei denn, sie bezahlten ein Lösegeld in Form der digitalen Währung BitCoin.

Eigentlich handelte es sich bei den Angriffen also um digitale Entführungen: Der Computer bleibt zwar stehen, aber die Festplatte ist weg, weil sie verschlüsselt worden ist. Auf Deutsch heissen solche Viren *Verschlüsselungstrojaner.* Weil dabei ein Lösegeld (englisch: *ransom)* gefordert wird, heissen sie auf Englisch *Ransomware.* Das Virus nistete sich über eine Netzwerkkomponente des Betriebssystems Windows auf den Computern ein. Betroffen waren vor allem ältere Windows-Rechner, die nicht mit dem von Microsoft kurz zuvor veröffentliche Sicherheitsupdate geschützt worden waren. Und das waren viele.

Experten sind alarmiert (wie immer)

Computerfachleute warfen ihre Stirn in Falten und warnten mit erhobenem Zeigefinger vor den Gefahren, die durch Viren und Trojaner drohen. Politiker und Experten warnten vor der Abhängigkeit von Computern und der unheilvollen Vernetzung. Der «Blick» bezeichnete WannaCry als *Megavirus* und warnte, der Trojaner könne jederzeit zurückkehren.[2]

Die Ereignisse schienen den Warnern recht zu geben. Im englischen Gesundheitssystem brach das nackte Chaos aus, wie NBC meldete.[3] Tausende von Untersuchungen und Operationen des staatlichen Gesundheitssystems NHS konnten nicht stattfinden, weil die Computer nicht mehr zur Verfügung standen. In Deutschland war der Verkehr der Deutschen Bahn beeinträchtigt. Reisende sahen auf den grossen Informationsdisplays in den Bahnhöfen statt Gleisnummern und Abfahrtszeiten die Lösegeldforderung der Hacker. Nicht auszudenken, was sonst noch alles hätte passieren können. Haben all die Menschen mit den erhobenen Zeigfingern also recht? Ist der Computer doch des Teufels? Führt und sie Abhängigkeit vom Computer ins grosse Abseits?

Wem nützt der Angriff?

Ach was. Die Geschichte vom grossen Cyberangriff lässt sich auch ganz anders lesen, wenn man bei allen Aussagen und Berichten jeweils, wie in einem Krimi, eine zentrale Frage stellt: *cui bono?* Wem nützt es? Die Berichte über Computerviren nützen zunächst einmal vor allem einer Branche: der IT-Sicherheit. All die Hersteller von Antivirenprogrammen, Firewalls und ähnlichen Produkten betreiben ein bigottes Geschäft: Mit der linken Hand warnen sie Dich vor bösen Hackern und Computerviren, mit der rechten Hand verkaufen Sie Dir den Schutz davor. Das ist so glaubwürdig, wie wenn eine Firma für Alarmanlagen Nachrichten über Einbrecher verbreitet.

Wem nützt es sonst noch? Die grosse Aufregung über den *Megavirus* und die Cybererpressung ist natürlich eine gute Story. Die Unsicherheit, die man damit verbreitet, verschafft Aufmerksamkeit. Ein Computervirus? Bin ich auch gefährdet? Was soll ich tun? Nebst der Sicherheitsbranche profitieren vor allem die Medien von weltweiten Gräuelgeschichten. Zumal sich eine solche Virenattacke problemlos in vier, fünf Häppchen aufteilen lässt: die Nachricht, die Schäden, Experten warnen, so können Sie sich schützen, die nächste Welle rollt. Auf diese Weise halten viele Medien die Aufregung (und damit die Klickzahlen) hoch. Und dann profitieren zu guter Letzt alle Technologiekritiker, die schon immer vor der Übermacht der Computer gewarnt haben.

Seit Jahren kein Service mehr

Aber halt, sagen Sie jetzt. In England sind tatsächlich Computer ausgefallen. In Spitälern! Das ist doch schrecklich.

Man stelle sich nur vor, was da alles hätte passieren können. Und das nur, weil wir Menschen zu sehr auf Computer vertrauen. Und die Deutsche Bahn. Man stelle sich vor, es trifft einen Flughafen. Oder die SBB. Furchtbar, was da alles passieren könnte. Da müssen wir doch Angst haben.

Beruhigen Sie sich. Dass der Verschlüsselungstrojaner im britischen Gesundheitssystem NHS so erfolgreich war, sagt vor allem viel über das NHS aus. Die englischen Spitäler sind so unterfinanziert, dass sie immer noch mit uralten Windows-XP-Systemen arbeiten. Das ist ein Betriebssystem, das Microsoft 2001 auf den Markt gebracht und 2008 eingestellt hat. Seit 2014 leistet Microsoft nicht einmal mehr Support für das System und veröffentlicht seither auch keine Updates mehr. Das System ist technisch tot. Wer trotzdem heute noch wichtige Computer im Betrieb hat, die mit Windows XP arbeiten, handelt grobfahrlässig. Das ist, wie wenn Sie mit einem Auto herumfahren, von dem Sie wissen, dass es seit Jahren nicht mehr zum Service in der Garage war.

Der wirkliche Skandal

Der wirkliche Skandal an der Geschichte ist nicht, dass einige Uraltcomputer in englischen Spitälern und schlecht gewartete Bildschirmsysteme der deutschen Bahn angegriffen wurden. Der Skandal ist, wie es zu dem Angriff kam. Die Hacker haben nämlich eine Sicherheitslücke ausgenutzt, die der amerikanische Geheimdienst NSA seit Jahren kannte. Statt Microsoft über die Lücke zu informieren, haben die NSA-Mitarbeiter die Lücke aber für sich behalten, damit sie sie selbst nutzen konnten. Möglicherweise hat Microsoft die Lücke auch auf Druck der NSA offengehalten. Ans Licht gekommen sind die Lücken, weil WikiLeaks geheime Hackerprogramme von CIA und NSA veröffentlicht hat. Microsofts Chefanwalt hat deshalb CIA und NSA für die erfolgreichen Angriffe auf die Windowssysteme mitverantwortlich gemacht.[4] Amerikas Sicherheitsdienste haben mit ihrem Verhalten wesentlich zur Unsicherheit der Computersysteme beigetragen.

Liegt das Problem also bei den Computern? Mitnichten. Die Menschen sind schuld. Die Verantwortlichen bei CIA und NSA, welche die Sicherheitslücke offenliessen. Die Zuständigen bei NHS und Deutscher Bahn, welche mit ungesicherten Uraltsystemen arbeiteten. Die Hacker, welche die Lücken ausnutzten.

Das Prinzip Verantwortung

Jetzt sagen Sie vielleicht, wir alle seien halt einfach überfordert. Für eine Privatperson sei es doch eine Zumutung, sich um all die Sicherheitspatches zu kümmern. Auch Profis kommen da nicht mehr mit. Die Gefahr liegt in der Komplexität der Computersysteme. Die Computer sind uns einfach über den Kopf gewachsen.

Ja, das kann schon sein. Auch die Politiker in England, die Bahnvorstände in Deutschland und die Privatanwender, die es traf, waren vielleicht einfach überfordert. Aber das enthebt sie alle doch nicht der Verantwortung. Auch der Computer ist, und sei er noch so kompliziert, nur ein Werkzeug. Wenn Sie mit einem Hammer jemandem den Schädel einschlagen, können Sie auch nicht sagen, der Hammer sei schuld. Die Verantwortung für ein Werkzeug haben Hersteller und Nutzer. Also die Menschen. Hören wir also auf, die Verantwortung auf die bösen, ach so komplexen Computer abzuschieben. Es ist der Mensch, der die Verantwortung trägt.

Ach ja, für den Fall dass Sie Ihre eigene Verantwortung übernehmen wollen, hier noch die drei Tipps, die Ihnen privat gegen WannaCry helfen:

1. Erstellen Sie täglich ein Backup Ihres Computers . Ja, täglich. Am besten automatisiert.
2. Installieren Sie Systemaktualisierungen immer sofort. Am besten auch automatisiert. Ja, das kann lästig sein. Aber es hilft.
3. Nutzen Sie keine Geräte, die Sie nicht wenigstens oberflächlich verstehen. Sie bleiben für Ihre Werkzeuge verantwortlich, auch wenn Sie keine blasse Ahnung haben.

Basel, 19.5.2017
mz@matthiaszehnder.ch

Quellen:

1 Siehe https://www.tagesschau.de/ausland/europol-wannacry-101.html

2 Siehe http://www.blick.ch/news/ausland/150-laender-bereits-betroffen-weltweite-cyber-attage-koennte-sich-noch-ausweiten-id6675241.html

3 Siehe http://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126

4 Siehe: http://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung