2017/21 Thema

https://jungle.world/artikel/2017/21/geheimdienste-haben-ein-interesse-sicherheitsluecken

Ein Gespräch mit Falk Garbsch, Sprecher des »Chaos Computer Clubs«, über digitale Sicherheit und Medienkompetenz

»Geheimdienste haben ein Interesse an Sicherheitslücken«

Interview Von **Julia Hoffmann**

Nach der weltweiten Cyberattacke der vergangenen Woche versuchen IT-Sicherheitsfirmen und Geheimdienste, die Urheber von Wannacry zu finden. Experten des Cybercrime-Zentrums von Europol sind überrascht vom Ausmaß des Angriffs. Der Informatiker und Software-Entwickler Falk Garbsch wundert sich kaum. Die »Jungle World« sprach mit dem Sprecher des »Chaos Computer Clubs« (CCC) über Sicherheitslücken, Medienkompetenz und über die Frage, weshalb gerade sensible Infrastrukturen schlecht geschützt werden.

Die Ransomware Wannacry hat in der vergangenen Woche Europol zufolge 200 000 Computer in 150 Ländern befallen. Die entsprechende Sicherheitslücke wurde mittlerweile geschlossen. Weiß man schon, woher das Virus kam?
Im Zweifel ist es schwierig herauszufinden, woher ein Virus kommt, denn jeder kann so etwas im Internet verbreiten, beispielsweise über Botnetze. Daher ist es ziemlich kompliziert zu ermitteln, wer den Code wann oder von wo gestartet hat. In der Vergangenheit wurde bei solchen Taten auch oft niemand dingfest gemacht. Das ist einfach so. An irgendeiner Stelle wird das Virus platziert und verbreitet sich dann selbst. Es nutzt den Rechner, um sich weiter zu verschicken, ehe es sich scharfschaltet und dann die komplette Festplatte des Computers verschlüsselt.

Es gab Spekulationen über eine nordkoreanische Urheberschaft.
Mit solchen Meldungen sollten wir sehr vorsichtig umgehen. Die Vermutungen basieren darauf, dass jemand bei der Analyse Codefragmente gefunden hat, die bereits früher in anderer Malware gefunden wurden. Diese wurde mit Nordkorea in Verbindung gebracht. Dieses Vorgehen ist aber eher Glaskugellesen als ein exakte Wissenschaft.

Welche Rolle spielt der US-amerikanische Geheimdienst NSA im Zusammenhang mit Wannacry?
Die Schwachstelle war der NSA bekannt und wurde offenbar von ihr auch genutzt. Die Geheimdienste haben ein großes Interesse daran, konkrete Informationen über Sicherheitslücken zu sammeln, um sie für sich zu nutzen. Sie können dann selbst Computersysteme angreifen und aushebeln sowie sich weltweit Zugang zu Systemen

verschaffen. Insbesondere für Zwecke der Industrie-, Wirtschafts- oder auch Wissenschaftsspionage werden diese Sicherheitslücken von Geheimdiensten genutzt.

Und wie funktioniert das?
Es gibt Sicherheitslücken, die auch dem Hersteller der entsprechenden Software oder des Betriebssystems nicht bekannt sind. Geheimdienste erwerben detaillierte Informationen über diese Lücken, behalten sie aber für sich und entwickeln passende Codes, die die Lücken ausnutzen und ihnen Zugang zu den Computern verschaffen. Das ist hier mit dem Erpressungstrojaner passiert.
Die NSA kannte die Sicherheitsücke bereits seit langer Zeit. Die Gruppe »Shadow Broker« hat der NSA diese und andere Informationen offensichtlich geklaut und sie dann veröffentlicht. Teil dieser Veröffentlichung war die Windows-Sicherheitslücke, die nun von Wannacry ausgenutzt wurde. Microsoft war das vermutlich auch schon einige Wochen vorher bekannt, denn es gab bereits im März einen Patch, um diese Lücke kurzfristig zu schließen. Sogar Sicherheitsaktualisierungen für nicht mehr unterstützte Windows-Versionen wurden später noch herausgegeben. Allerdings hätte das viel früher passieren können, wenn die NSA Microsoft von der Sicherheitslücke rechtzeitig in Kenntnis gesetzt hätte.

Microsoft hat sich auch schon über die verzögerte Meldung beschwert.
Die Rechtsabteilung will sich natürlich gegen mögliche Schadenersatzzahlungen absichern. Außerdem ist es für Softwarehersteller schon ein Problem, Sicherheitslücken zu entdecken und zu schließen. Da ist man darauf angewiesen, dass Leute solche Lücken finden und sie den Herstellern dann auch melden. Und weil solche Sicherheitslücken eine Gefahr für wichtige Infrastrukturen bedeuten können, sollte es auch eine Verpflichtung geben, Sicherheitsprobleme zu melden. Das fordern wir bereits seit Jahren. Gerade Geheimdienste sollten das tun. Trotzdem hätte Microsoft das Problem auch besser an seine Kunden kommunizieren müssen.

Gibt es Infrastrukturen, die besonders von den Angriffen betroffen waren?
Es handelt sich hier um keine gezielten Angriffe. Die NSA und andere Geheimdienste hätten da sicher anders agiert und gezielt Institutionen oder Betriebe angegriffen. Die betroffenen Rechner benutzen alle ein Betriebssystem von Windows und da werden häufig nicht alle Sicherheitsupdates und Aktualisierungen eingespielt. Größere Netzwerke und Privatnutzer sind besonders anfällig. Die Deutsche Bahn hat es beispielsweise getroffen, aber auch Krankenhäuser. Im schlimmsten Fall kann so etwas aber auch ganze Industrieanlagen betreffen. Besonders dort ist teilweise sogar noch das alte Windows XP in Benutzung.

Weshalb werden diese sensiblen Infrastrukturen nicht besser geschützt?
Gerade in Krankenhäusern, wo große Maschinen wie Ultraschall-, MRT- oder CT-Geräte im Einsatz sind, werden diese immer weiter vernetzt und besonders hardwarenah in die Infrastruktur eingebunden. Das heißt, wenn man ein Windows-Update macht, muss man damit rechnen, dass die Maschine teilweise nicht mehr funktioniert oder auch ganz ausfällt. Das haben ja viele Nutzer schon privat erlebt: Nach dem Update funktioniert irgendetwas nicht mehr. Für die Krankenhausinfrastruktur ist es natürlich besonders kritisch, wenn etwas ausfällt. Deshalb spart man im Zweifel an den Updates. Das ist Sparsamkeit an der falschen Stelle, weil so diese eklatanten Sicherheitslücken nicht behoben werden.

Sie setzen sich immer wieder für eine gezielte Förderung von Medienkompetenz ein. Muss es auch eine neue Sicherheitskompetenz im Netz geben?

Wir tendieren dazu, auf die großen Konzerne und die Politik zu zeigen, die die Probleme beheben sollen. Dabei wissen wir selbst, dass man nicht auf jeden E-Mail-Anhang klicken sollte. Die Leute machen es aber trotzdem und infizieren ihre Rechner und damit auch andere Computer. Wir kennen die Gefahren und Risiken im Internet, aber haben sie offenbar noch nicht genügend verinnerlicht. Da muss es eine kulturelle Veränderung und ein Umdenken geben. Das sollte am besten auf verschiedenen Ebenen passieren. Dafür muss mehr Medienkompetenz in die Schulen und Universitäten. Nicht als Unterrichtsfach, sondern als Querschnittskompetenz. Wenn wir das vor zehn Jahren getan hätten, hätten wir möglicherweise die Debatten über fake news heute gar nicht.
Dennoch darf man sich auch nicht verunsichern lassen durch politische Worthülsen wie Cyberwar und Cyberwehr, die Bedrohung suggerieren. Diese Verunsicherung spielt Rechtspopulisten in die Hände und führt dazu, dass man auf ergebnisorientierte Politik verzichtet, statt auf Fachleute zu hören.

Europol und das britische Zentrum für Cybersicherheit haben davor gewarnt, dass die Auswirkungen der Attacke noch deutlich größer werden könnten. Wie geht es weiter?
Wir werden sehen. Es gibt mittlerweile eine neue Variante des Virus. Üblicherweise dauert das aber, bis eben jeder und jede die Sicherheitsupdates eingespielt haben. Da ist jeder selbst in der Pflicht. Natürlich profitieren am Ende alle davon, wenn man Sicherheitslücken schließt. Und auch die Politik muss verstehen, dass hier kein nationales Problem vorliegt, sondern ein internationales.