WARUM DIE CYBER-SICHERHEITSKULTUR EIN UPDATE BRAUCHT

Aktualisiert am 3. Jul. 2017 Von Thea Kommentieren

von Thea Riebe und Jens Geisse

Ransomware wie WannaCry und Petya/NotPetya[1] versetzten weltweit Unternehmen in Sorge und verursachen erheblichen Schaden. Dabei sind sie nur der sichtbare Teil einer unzureichenden Sicherheitskultur, die dringend ein Update benötigt.

Ransomware, auch Kryptotrojaner genannt, sind kein neues Phänomen, sondern die zunehmend sichtbare Begleiterscheinung kollektiver IT-Unsicherheit. Die Ransomware WannaCry infizierte Mitte Mai weltweit mindestens 220.000 Windows Rechner. Dabei verschaffte sich der Trojaner Zugang zu den Dateien der Computer und verschlüsseln diese um eine Lösegeldzahlung zu erpressen.

Dies war möglich über die als EternalBlue bekannte Lücke, die seit dem Betriebssystem Windwos XP auftrat und erst in diesem Jahr im Februar durch Microsoft geschlossen wurde. EternalBlue war für eine unbekannte Zeit in den Händen der NSA bis sie Anfang dieses Jahres durch eine Hackergruppe namens Shadow Brokers von der NSA „gestohlen“ und veröffentlicht wurde. Und obwohl Microsoft eiligst einen Patch veröffentlichte, offenbarten die bisher folgenreichsten bekannte Kryptowurm das Dilemma, in dem sich die Cyber-Sicherheitskultur aktuell befindet: Es ist eine Kultur des Schweigens, die dazu führt, dass das Sammeln und der Missbrauch von Sicherheitslücken gefördert statt verhindert wird.

Der Zahlungsverkehr auf die Bitcoin Konten von WannaCry wurde durch einen automatischen Twitterfeed automatischen Twitterfeed sichtbar gemacht. Dort lässt sich sehen: Es gibt immer noch Opfer, die bezahlen. Trotz der öffentlichen Aufklärung und des Vorhandenseins eines Patches. Microsoft spricht daher weiterhin von einem „erhöhtem Risiko“ für seine Kunden und stuft die Nutzung von Windows XP als unverantwortbar ein. Und während diese Ransomware öffentliche Aufmerksamkeit erfahren hat, bleibt verborgen, wie viele Unternehmen, Behörden, und Bürger von Spionage-Software betroffen sind, die jahrelang genau die selbe Lücke genutzt haben könnte und teilweise immer noch nutzen kann.

Diese anhaltenden Attacken auf bekannte und gepatchte Schwachstellen und die Reaktion von Microsoft zeigen, dass

Sicherheitspatches für aktuelle Betriebssysteme bei weitem nicht ausreichen, sondern dass es eine Sicherheitskultur braucht, in der unterschiedliche Sicherheitssysteme zusammenwirken und sich gegenseitig absichern. Es reicht nicht aus, Updates zu veröffentlichen, sondern sie müssen auch installiert werden, und von anderen Maßnahmen, wie z.B. verschlüsselten Backups, begleitet werden. NotPetya hat sich sogar über ein kompromittiertes Update installiert und wurde auf diesem Weg verbreitet. Daran lässt sich erkennen, dass es kein alleiniges Mittel für mehr Sicherheit gibt, sondern nur Teil einer umfassenden Sicherheitskultur sein kann, für die auch staatliche Behörden durch ihr Handeln eine Mitverantwortung tragen. Microsoft gab in einem einmaligen Schritt der NSA die Schuld an den Folgen von WannaCry, und setzte das Wissen um diese Lücken mit dem Besitz von konventionellen Waffen, wie Raketen gleich:

> *“Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles*

> *stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action."*[2]

Die unintendierte Kooperation von Staaten und Cyber-Kriminellen wird durch eine Kultur des Schweigens gefördert, weil Staaten und Kriminelle die Sicherheitslücken jeweils für sich nutzen wollen. Staatliche Akteure nutzen entdeckte Lücken, um entweder andere Staaten auszuspionieren, oder Bürger und Unternehmen unbemerkt überwachen zu können. Cyber-Kriminelle profitierten vielfältig von dem mangelnden Interesse von Staaten diese Lücken zu schließen, unter anderem indem sie das Wissen um die Sicherheitslücken an Staaten verkaufen, Wirtschaftsspionage betreiben oder die Rechner für eigene Zwecke, zum Beispiel als Teil eines Botnets verwenden. Aber auch die Unternehmen profitieren vom Schweigen: Als Opfer fürchten sie einen Vertrausverlust ihrer Kunden und als IT-Sicherheits- oder als Softwaredienstleister profitieren sie davon, dass die

Unternehmen sich einzeln und im Geheimen an sie wenden, anstatt kollektive Lösungen zu finden.

Microsoft fordert deshalb die völkerrechtliche Regulierung von staatlichen Cyber-Attacken und dem Stockpiling der Exploits durch eine „Digital Geneva Convention“:

> *“For two-thirds of a century, since 1949, the world’s nations have recognized through the Fourth Geneva Convention that they need to adhere to rules that protect civilians in times of war. But nation-state hacking has evolved into attacks on civilians in times of peace.”*[3]

Und auch andere Organisationen und Experten fordern gesetzliche Normen, die zum Offenlegen von Softwarelücken verpflichten, wie der Chaos Computer Club (CCC) und das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF). Auch auf dem IT-Sicherheitskongress

des BSI im Mai 2017 forderten die Experten daher eine Meldepflicht für Sicherheitslücken gesetzlich zu verankern.

Was kann politisch gegen diese Kultur der Cyber-Unsicherheit getan werden? Und wie lässt sich trotz der Unzulänglichkeit einzelner Maßnahmen eine resiliente Sicherheitskultur etablieren? Updates für aktuelle Software alleine reichen nicht aus, sondern können sogar selbst Schadsoftware verbreiten, wenn der Updatemechanismus kompromittiert wird. Auch mit sicherer Software bleibt das Problem von “social engineering",[4] das heißt das Ausnutzen menschlichen Verhaltens als Angriffsstrategie bestehen, das auch in der Sicherheitskultur aufgegriffen werden muss.

Um die aktuelle Cyber-Unsicherheitskultur abzulösen, sollte die politische Debatte folgende Punkte aufgreifen:

1. Cyber-Attacken betreffen fast ausschließlich zivile Strukturen. Ihr Einsatz durch Staaten lässt sich deshalb kaum legitimieren. Wir brauchen eine Diskussion darüber, welches Handeln staatlicher Akteure inakzeptabel ist. Wie Brad Smith (Microsoft) richtig anmerkt, werden Zivilisten durch die Genfer Konventionen geschützt, und dies muss auch für digitale Kampfhandlungen gelten.
2. Stockpiling erhöht die Verwundbarkeit digitaler Infrastrukturen. Wenn bekannte Sicherheitslücken verschwiegen werden, reduziert dies zwangsweise die Sicherheit vor Cyber-Attacken. Stockpiling durch staatliche Institutionen, welche eigentlich die Sicherheit

erhöhen sollen, wird dadurch besonders ambivalent. Die erneute Diskussion über Staatstrojaner zur Quellen-TKÜ muss dies aufgreifen: Neben rechtsstaatlichen Bedenken ist es durchaus denkbar, dass solche Eingriffe die Sicherheit in der Summe herabsetzen.

3. Die Anreize in unserer momentanen Sicherheitskultur sollten evaluiert werden. Wenn Organisationen davon profitieren, oder zumindest weniger Schaden nehmen, wenn erfolgreiche Angriffe nicht öffentlich gemacht werden, kann kaum vernünftig auf Gefahrenpotentiale reagiert werden. Dies ist besonders wichtig im Hinblick auf die Zunahme der Smart Devices, Industrie 4.0 und das Internet der Dinge. Zu einer effektiven Sicherheitskultur gehören notwendigerweise Anreize für sicherheitsförderndes Verhalten.

Thea Riebe ist Studentin der Internationalen Studien/Friedens- und Konfliktforschung an der Goethe Universität Frankfurt sowie der TU Darmstadt und arbeitet als studentische Mitarbeiterin bei der Forschungsplattform IANUS an der TU Darmstadt.

Jens Geisse studierte Soziologie und Informatik in Marburg und Darmstadt, promoviert in der Technikphilosophie zum Begriff des Programms, und arbeitet als Koordinator bei der Forschungsplattform IANUS an der TU Darmstadt.

Die Autoren danken der freundlichen Hilfe von Martin Schmetz bei der Korrektur.

1. Dabei ist NotPetya inzwischen als ein möglicherweise politisch motivierter Trojaner eingestuft worden, der sich als Ransomware getarnt hat. Da er sich durch ein Update der Ukrainischen Steuersoftware MeDoc vor allem zunächst in der Ukraine verbreitete, vermutet die Ukraine russische Akteure hinter der Attacke. ↩
2. Brad Smith, The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack, 14. Mai 2017. ↩
3. Brad Smith, The need for a Digital Geneva Convention, 14. Februar 2017. ↩
4. "Just a few minutes ago, before I came on stage, somebody here in the audience tweeted that every company has at least one employee that will click on anything. That's why 90 percent of intrusions begin, unfortunately, with a phishing email." Brad Smith, Transcript of Keynote Address at the RSA Conference 2017 "The Need for a Digital Geneva Convention". ↩

Tags: Cyber Security cyber sicherheit Cyber Spionage Cybercrime Hacken Industrie 4.0 Sicherheitskultur Stockpiling

SCHREIBE EINEN KOMMENTAR

Deine E-Mail-Adresse wird nicht veröffentlicht.

Kommentar

Name

E-Mail

Website

Ich bin kein Roboter.
reCAPTCHA
Datenschutzerklärung - Nutzungsbedingungen

Kommentar abschicken

Benachrichtige mich über nachfolgende Kommentare per E-Mail.