Newsletter für Engagement und Partizipation in Deutschland
11/2021

Teresa Staiger

Wine & Hack – mit Spaß und Humor zu mehr Sicherheit

Datensicherheit kann Spaß machen!

»IT- Sicherheit und Spaß – das schließt sich schon grundsätzlich aus? Stimmt nicht, sagen wir« war der Untertitel der Veranstaltung »Wine & Hack« des »Forum Digitalisierung und Engagement«. Und wie Recht wir damit hatten: der Vortrag von Götz Sattler, IT'ler und, wie er sich selbst nennt, «Hacker», war kurzweilig, sehr informativ und hat die Augen vieler Teilnehmer*innen geöffnet.

Anlässlich der dritten Dialogphase »Datenschutz und Datensicherheit« war das Ansinnen der Veranstaltung, sich die Relevanz von Datenschutz und Datensicherheit durch eine praxisnahe und eben humoristische Demonstration zu vergegenwärtigen. Wir alle sind tagtäglich mit Laptops und Handys im Netz, wir kommunizieren und arbeiten online. Dennoch gerät der Datenschutz und die Datensicherheit oftmals wegen ihrer trockenen Images ins Hintertreffen. Doch IT-Sicherheit muss nicht zwangsläufig langweilig sein, es kommt nur darauf an, wie man das Thema angeht. Götz Sattler (»Die Hackershow«) zeigte in anderthalb Stunden auf eindrucksvolle, aber amüsante Art und Weise, wie wichtig Datenschutz und Datensicherheit im Netz ist. Durch Beispiele wurden die Teilnehmer*innen kurzweilig für Informationssicherheit sensibilisiert, indem er etwa zeigte, wie leicht Handys und Sicherheitslücken genutzt und Ihre Daten ausgespäht werden können und wie man dies zukünftig verhindern kann.

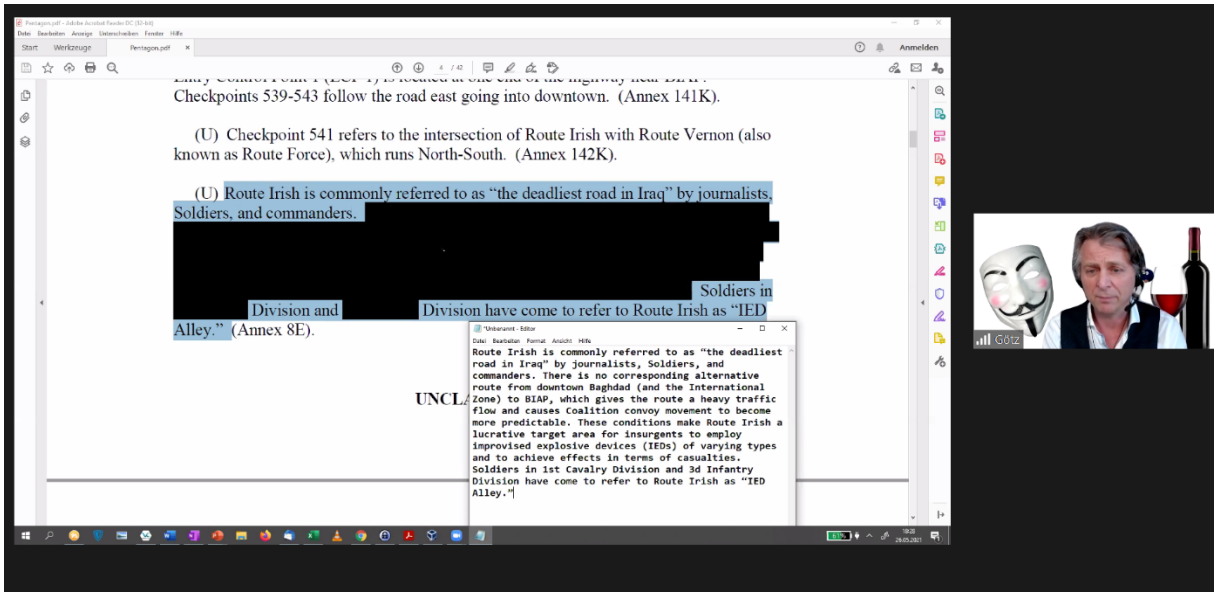
Nach einer kurzen Einführung in das Thema und der Erkenntnis, dass Hacker*innen natürlich nicht nur Mittzwanziger mit hohem Mate- und Pizzakonsum sind, also nicht ganz dem Klischee entsprechen, dass man sich so vorstellt, wurde deutlich, dass es durchaus ein professionelles und lukratives Geschäft sein kann, nebenher oder hauptberuflich zu hacken. Denn salopp gesagt: Das Datenkidnapping ist sehr viel weniger aufwändig als das klassische Kidnapping.

Was genau ist überhaupt ein Hack?

Im weitesten Sinne wird ein technisches System so umfunktioniert, damit es etwas anderes tut als vorgesehen. Wau Holland, der Mitbegründer vom Chaos Computer Club, sagte einmal: »Ein Hacker ist jemand, der versucht einen Weg zu finden, wie man mit einer Kaffeemaschine Toast zubereiten kann!«. Ein gutes Beispiel für diese Analogie ist John Thomas Draper, auch Captain Crunch genannt, der mit einfachsten Mitteln, nämlich mit einer Plastikpfeife aus einer Cornflakes-Packung, das Telefonsystem so hackte, dass man gratis telefonieren konnte. So kam er also zu seinem Spitznamen.

Soviel zum Hintergrund. Was hat das nun mit Informationssicherheit zu tun? Grundwerte der Informationssicherheit sind Vertraulichkeit, Verfügbarkeit und Integrität der Daten. Wie werden diese Grundwerte konkret angegriffen und was ist die Motivation dahinter? Die Gründe sind vielfältig und reichen von Ruhm/Ego/sportlichem Ehrgeiz über politische Motivation (Hacktivisten) bis zu Kriminellen mit finanzieller Motivation. Aber auch Sicherheitsberater*innen, die Sicherheitslücken finden sowie Cybersoldat*innen gehören zum Hackuniversum.

Die Arten von Angriffen rangieren von Ausnutzen von Benutzerfehlern über ungezielte Angriffe wie z.B. Spam-Mails bis zu gezielten Angriffen. Götz Sattler zeigte einen sehr einfachen Benutzerfehler, bei dem alle mit grundlegenden Computer-Skills ganz schnell zu Hacker*innen werden können. Und zwar hatte das Pentagon eine PDF-Datei eines Einsatzberichtes aus dem Irak mit mehreren geschwärzten Passagen ins Netz gestellt. Nun konnte man aber ganz leicht über Strg C und Strg V den Text markieren und in den Editor kopieren – und zack, der Fließtext wurde trotz geschwärzter Passagen komplett lesbar. Dieses Beispiel zeigt, dass sogar ein einfaches Textbearbeitungsprogramm sehr anfällig sein kann, eben je nach Anwendung oder Anwender*innen. Sattlers Tipp: lieber den Text ganz rauschlöschen, somit kann auch kein Text herauskopiert werden. ;-)



(Bild von der Veranstaltung »Wine & Hack«)

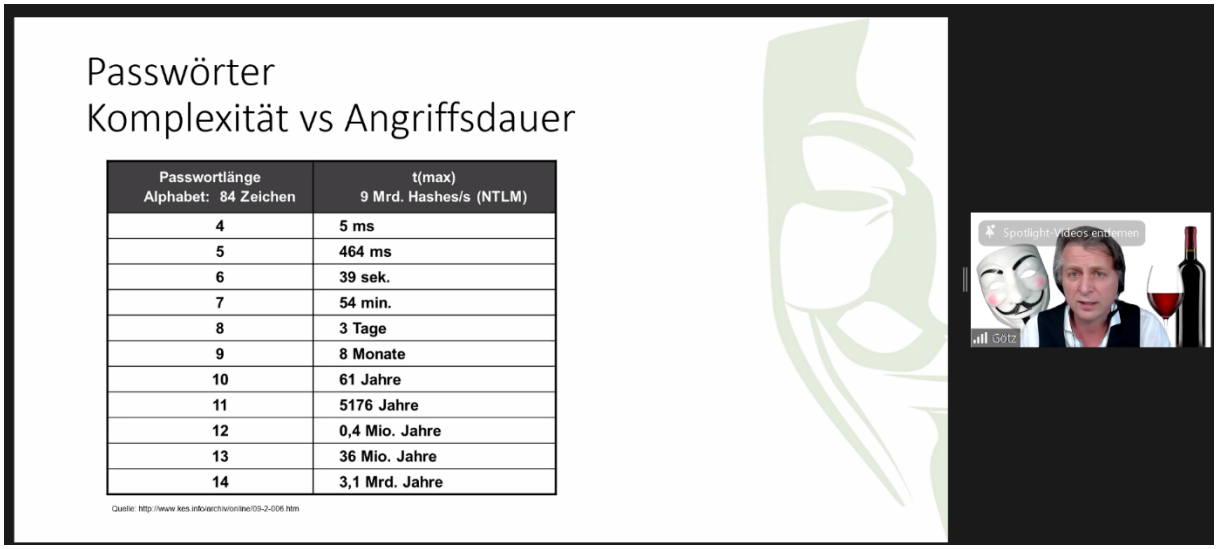
Was ließ sich sonst noch lernen?

Weitere Benutzerfehler sind etwa Metadaten in Word-Dokumenten sowie GPS-Daten in Bildern. So gibt man unbewusst Daten frei, die dann wiederrum ausgenutzt werden können.

Götz Sattler zeigte darüber hinaus auch Beispiele für ungezielte Angriffe: etwa das Phishing mit dem Ansinnen, Passwörter zu klauen. In diesem Fall können Sie Hack-Attacken ein Schnippchen schlagen und auf Webseiten wie https://haveibeenpwned.com/ und https://sec.hpi.de/ilc/ vom Hasso-Plattner-Institut herausfinden, ob Ihre Daten in Leaks aufgetaucht sind.

Das einfachste Mittel, um es Phishing-Attacken schwer zu machen, ist denkbar einfach: gute und vor allem lange Passwörter. Denn je länger sie sind (alles ab 12 Zeichen ist schon mal gut!), desto sicherer sind sie gegen Phishing-Angriffe.

Auch demonstrierte Götz Sattler eindrucksvoll, wie einfach es ist, aus gekaperten Hashwerten die dahinterliegenden Passwörter zu ermitteln. Dafür braucht ein*e Angreifer*in nur ein (frei zugängliches) Programm, eine gute Grafikkarte und einen anständigen Prozessor. Natürlich haben professionelle Hacker*innen noch anspruchsvollere Systeme und besseres Equipment, es verdeutlicht dennoch, wie einfach es sein kann, Passwörter zu knacken.



(Bild von der Veranstaltung »Wine & Hack«)

Weitere ungezielte Angriffe laufen unter anderem über Portscans, (Spear-) Phishing-Mails mit verseuchten Links oder Drive-by-Dowloads. Götz Sattler nannte vier einfache Maßnahmen, die laut Bundesamt für Sicherheit in der Informationstechnik (BSI) bis zu 98% Schutz vor ungerichteten Angriffen bieten: Virenscanner aktiv und aktuell halten, Firewall nicht ausschalten, Betriebssysteme und Programme updaten und nicht permanent mit Adminrechten arbeiten.

Ein weiteres Beispiel, dafür wie Hacken immer mehr durch perfides Social Engineering erfolgreich wird, war der Trojaner »Goldeneye«, der Bewerbungen auf ausgeschriebene Stellen mit Lebenslauf im Anhang an unzählige Personalabteilungen schickte. Durch Worddateien mit Makros wurden dann die Laufwerkverzeichnisse verschlüsselt. Ein Makro ist eine Kette von Befehlen in einem Anwendungsprogramm. Es dient der Automation von Funktionen und kann deshalb auch als Unterprogramm bezeichnet werden. Generell gilt: Makros von unbekannten Quellen nicht ausführen.

Zum Schluss demonstrierte Götz Sattler, wie auch Smartphones zu Schwachstellen werden, da sie in der Regel ziemlich viel über einen wissen: E-Mails und Instant Messenger, Zugangsdaten, Kalendereinträge, vorherige Standorte, Fotos, Kontakte, Browserverlauf etc. Durch einen Smartphone-Trojaner (Kostenpunkt 350 $) zeigte er, was man als Angreifer*in alles zu sehen bekommt. Kurz gesagt: alles. Die letzten Anrufe, die letzten SMS, alle Tastatureingaben,

den aktuellen Standort, das Bewegungsprofil, Fotos und es lässt einen sogar bei Telefonaten lauschen.

Was hilft gegen solche Trojaner und andere Angriffe?

Im oben genannten Beispiel ist das ganz einfach: das Endgerät (hier das Smartphone) sperren, es reichen nämlich 10 Minuten ungesperrter Zugriff auf das Handy, um an eine Vielzahl sensibler Daten zu gelangen. Gebrauchte Smartphones sollten daher bei Wiederverkauf oder Nichtmehrverwendung immer auf Werkseinstellungen zurückgesetzt werden. Auch bei Apps lässt sich die Sicherheit erhöhen, z.B. durch eingeschränkte Rechte. Kleiner Tipp: Nach der Lektüre dieses Artikels schauen Sie doch einfach mal, welche Apps Sie deinstallieren könnten, welche Rechte diese beanspruchen und ob der Zugriff in dem Fall notwendig ist.

Nach anderthalb Stunden geballter Sensibilisierung für Informationssicherheit mit den Beispielen aus der Praxis, blieb noch Zeit für einen Drink und Schnack mit anderen Engagierten. Die Veranstaltung hat gezeigt: »Technologie muss man nicht bekämpfen, sondern beherrschen«, um mit Wau Hollands Worten zu schließen.

Autorin

Teresa Staiger *ist Referentin im Projekt »Forum Digitalisierung und Engagement« des BBE. Zuvor war sie am Max-Planck-Institut für Intelligente Systeme tätig. Sie hat ihr Studium an der Johannes-Gutenberg-Universität Mainz und Cardiff University (B.A. Politikwissenschaft und Geschichte) und an der Philipps-Universität Marburg (M.A. Politikwissenschaft) absolviert. Sie interessiert sich besonders für eine gemeinwohlorientierte Digitalisierung, die durch eine digital souveräne und engagierte Zivilgesellschaft begleitet wird.*

Kontakt: *teresa.staiger@b-b-e.de*

Forum Digitalisierung und Engagement:

Kontakt: info@forum-digitalisierung.de

Website: www.forum-digitalisierung.de

Twitter: @BBE_Forum

Redaktion

BBE-Newsletter für Engagement und Partizipation in Deutschland
Bundesnetzwerk Bürgerschaftliches Engagement (BBE)
Michaelkirchstr. 17/18
10179 Berlin
Tel: +49 30 62980-115

newsletter@b-b-e.de
www.b-b-e.de