Digital angreifbar und doch wehrhaft - vom trauten Heim, über die Fertigungsstraße bis zum Hochsicherheitstrakt

Staatstrojaner und böse Trojaner

Nur wenige Abgeordnete waren an diesem heißen Sommertag im Bundestag, als lässig der Staatstrojaner durchgewunken wurde. Viele Volksvertreter glänzten bei der Debatte um Bastionen der Freiheitlich Demokratischen Grundordnung durch Abwesenheit.

Während sie nicht dabei waren, wurde mit dem Argument der Terrorbekämpfung die Möglichkeit zur Online-Durchsuchung privater Computer und Telefone auf einen Katalog von insgesamt 27 Delikten in der alltäglichen Strafverfolgung ausgeweitet - bis hin zur "Verschleierung unrechtmäßig erlangter Vermögenswerte".

Versteckt wurden die Attacken auf die FDGO in einer „Formulierungshilfe“ zu zwei Gesetzentwürfen, in denen es um DNA-Abgleiche und Fahrverbote für Straftäter geht. Das bedingte Amüsement über den Umgang mit „bösen“ und „guten“ Trojanern steigt indes, nicht nur beim Chaos Computer Club, zum denkbar schlechten Zeitpunkt.

Digitale Verletzlichkeit wird ausgenutzt

Die Digitalisierung von Wirtschaft und Gesellschaft macht verletzlich. ……

…….

Microsoft-Manager Brad Smith warnte am 14. Mai in einem Blogbeitrag zu WannaCry vor dem Verlust hochwirksamer Cyberwaffen aus Regierungsbeständen: „Ein vergleichbares Szenario bei konventionellen Waffen wäre es, wenn dem US-Militär Tomahawk-Raketen geklaut worden wären."

Ähnlich sieht das SySS-Geschäftsführer Sebastian Schreiber, erfolgreicher Auftragshacker im Dienste von Unternehmen, die ihre Sicherheitslücken aufdecken wollen: „Die NSA kennt die Windows-Schwachstelle, auf der die Weiterverbreitung des Trojaners fußt, schon seit vielen Jahren. Anstatt die Sicherheitslücke an den Hersteller zu melden, wurde diese geheim gehalten, um so über Hoheitswissen zu verfügen und anhand dieses Wissens selbst Windows-Systeme knacken zu können.“

…..

Security, also Sicherheit, hat in der Digitalisierung viele Gesichter und Konfliktfelder. In Deutschland soll die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ (Zitis) Methoden entwickeln oder ausfindig machen, mit denen Polizei und Verfassungsschutz codierte Messenger-Dienste wie Whatsapp knacken und verschlüsselte Mitteilungen lesen oder mithören. Ebenfalls zum Bundesinnenministerium gehört das Bundesamt für Sicherheit und Informationstechnik (BSI). Seine Aufgabe ist es, Schwachstellen in der Kommunikation und

Sicherheitslücken im Internet aufzuspüren und die Bürger davor zu warnen, statt sie selbst zu nutzen, wie Zitis. Eine interessante Konstellation.

Bei behäbigen Strukturen extern und in den Wolken sichern

Maschinelles Lernen, Künstliche Intelligenz, mathematisches Nachspüren allein reichen nach Ansicht von Sicherheitsexperten wie Thomas Uhlemann von ESET jedoch nicht aus, um Erpressersoftware und Schadsoftware rechtzeitig aufzuspüren. Mehrschichtige Systeme und aufmerksame, geschulte Menschen müssen die digitalisierte Lebens- und Arbeitswelt gemeinsam verteidigen.

Angriffe auf vernetzte Geräte, die dann nicht mehr funktionieren, inklusive Fahrzeugen, Türsystemen, Thermostaten, oder Geiselhaft für verschlüsselte, vertrauliche Daten werden nach Prognosen von ESET zunehmen. … Kritische Infrastrukturen in Krankenhäusern sind durch Vernetzung anfällig, besonders wenn für sie kein ausreichendes Sicherheitsbudget vorgesehen ist.

…..

Ob Produktionsmaschinen in Fertigungsbetrieben, Medizintechnik oder Automobilbranche – alte Systeme wie Windows XP sind dort oft noch zuhause, weil die Geräte auf Jahrzehnte halten müssen oder die Compliance-Regularien extrem streng ausgelegt werden. Eine Umstellung ist aufwändig, teuer, unbequem oder gar unmöglich.

……

Auch kleine und mittlere Unternehmen könnten durch Erpressersoftware und Verschlüsselung schnell lahmgelegt werden. „Wenn der Zugriff auf Daten nicht möglich ist, kann kein Angebot geschrieben werden, kein Auftrag bearbeitet werden. Letztlich ist ein Unternehmen, je nach Kalkulation, nach wenigen Tagen kurz vor der wirtschaftlichen Katastrophe“, sagt Andreas Schlechter, Geschäftsführer von Telonic, einem Kölner Unternehmen, das als Systemhaus auf Network und Security spezialisiert ist.

…

Hacking macht nicht an der Haustür halt

Die Nutzer müssten auch in Smart Homes oder Smart Cars sensibel feststellen, ob sie noch mit ihrem ursprünglichen Gerät reden oder gerade manipulierte Sensoren untergeschoben bekommen, …Sie sollten wissen, dass Mikrofone und Kameras in Fernsehern, Computern und smarten Assistenten auch ihr Privatleben in die Ferne und zu ungewollten Beobachtern übertragen könnten. Sie sollten darüber aufgeklärt werden, wie sie sich wehren und wie sie die benötigten Funktionen erhalten, wenn etwa die Hausinfrastruktur attackiert wird.

….

Wenn von außen die Webcam „übernommen“ wird, kommt der Angreifer so doch nicht an die Gasheizungssteuerung. …

Text: Annegret Handel-Kempf

Fotoquelle: Annegret Handel-Kempf