Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 182 (2016)

Heft: 10

Artikel: Cyber-Attacken als akute Gefahr

Autor: Ruef, Marc

DOI: https://doi.org/10.5169/seals-630312

Cyber-Attacken als akute Gefahr

Cybersecurity ist ein topaktuelles Thema, das aus unserer Gesellschaft nicht mehr wegzudenken ist. Neben wirtschaftlichen Auswirkungen von Cybercrime führt das Thema Cyberwar auch eine militärische Relevanz mit sich. Die gegebenen Risiken können nicht einfach so ausgeblendet werden. Vor allem, wenn man bedenkt, was die Zukunft noch alles bringen wird.

Marc Ruef

Nicht erst mit dem Zwischenfall der RUAG im Mai dieses Jahres hat das Thema Cybersecurity an Brisanz gewonnen. Angriffe auf kritische Infrastrukturen und die Möglichkeiten der digitalen Kriegsführung sind dadurch aber vermehrt ins Bewusstsein der Allgemeinheit getreten. Die damit einhergehenden Überlegungen sind aber nicht nur dem militärischen Sektor vorbehalten. In einer von Technologien getriebenen Gesellschaft ist mittlerweile jeder den vielschichtigen Risiken im digitalen Raum ausgesetzt.

Angriffe auf Computersysteme werden in der Privatwirtschaft als konkrete und alltägliche Gefahr wahrgenommen. In grossen Firmen sind oftmals mehrere Teams darum bemüht, die Bedrohung zu erkennen und damit verbundene Risiken einzuschätzen. Durch gezielte Sicherheitsüberprüfungen, sie werden Penetration Tests genannt, sollen Schwachstellen in exponierten und kritischen Systemen gefunden werden. Dies ist nicht mehr nur ein Steckenpferd von ein paar Enthusiasten: Mittlerweile hat sich auf der Basis dieser Vorgehensweise eine hochprofessionalisierte Industrie gebildet.

Markt für Angriffstools

Schwachstellen in Computersystemen können zu grossen Schäden führen, die nachweislich Schäden in Bezug auf Reputation und Wirtschaftlichkeit sowie juristische Auswirkungen auf eine Organisation haben können. Und Angriffe werden längst nicht mehr nur durch jugendliche Lausbuben, den sogenannten Skript-Kiddies, angestrebt.

Im Darknet, dem digitalen Untergrund des Internets, existiert ein florierender Markt für den Austausch von Angriffstools, den sogenannten Exploits. Wer im Besitz eines scharfen Exploits ist, kann mit einem simplen Klick eine Schwachstelle ausnutzen. Technische Hintergründe, die zu erwerben langwierig sind, sind dem Angreifer dank eingekauftem Exploit egal. Das Entwickeln dieser Exploits ist aufwendig, weshalb sie teilweise für viel Geld gehandelt werden. Die Preisstruktur ist dabei komplex, orientiert sich jedoch in erster Linie an Popularität des angegriffenen Produkts und den Möglichkeiten einer erfolgreichen Attacke.

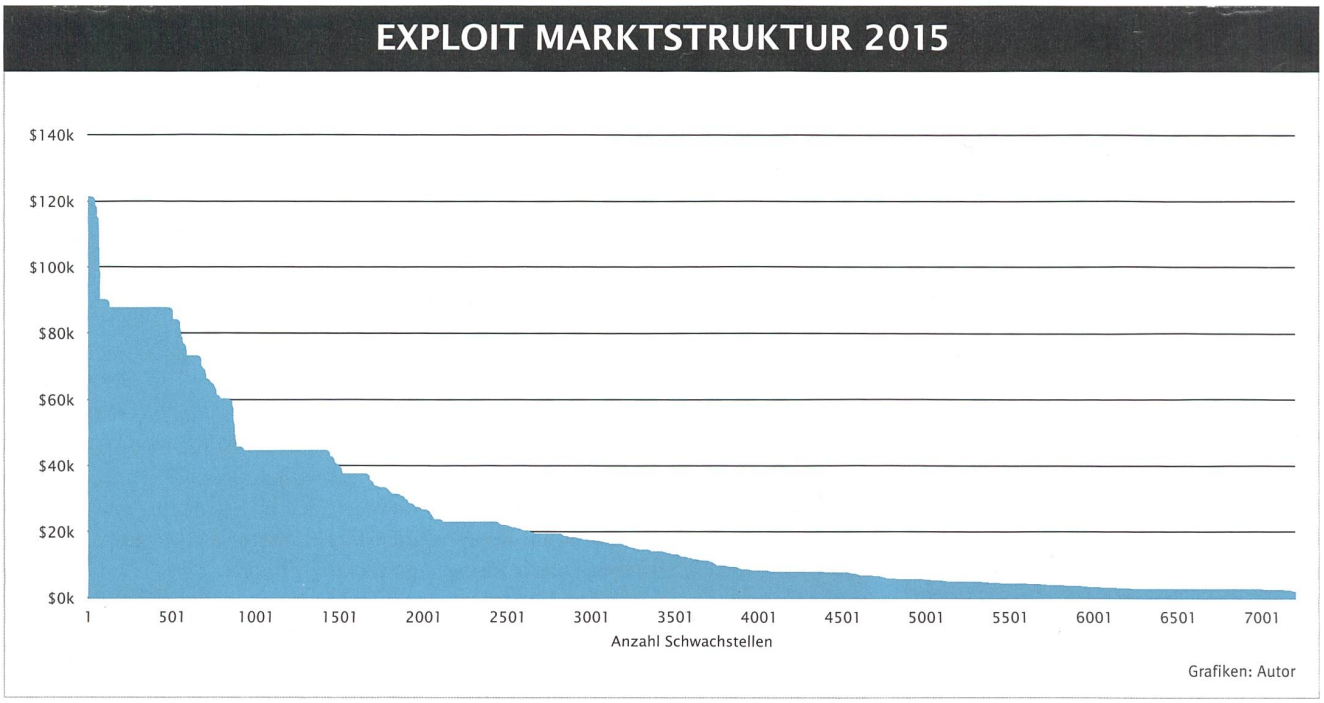
Rekordpreise werden für iPhone-Exploits bezahlt. Im September 2015 wurde zum ersten Mal der Verkauf eines Exploits für 1 Mio. USD bestätigt, und Mitte 2016 wurde der Rekord erneut mit 1,2 Mio. USD gebrochen. In diesen Preisregionen bewegen sich in erster Linie nachrichtendienstliche Akteure mit entsprechend aufgestocktem Budget.

Das Marktvolumen im Exploit-Umfeld wachst jährlich und ist in den letzten Jahren regelrecht explodiert. Dies lockt interessierte Forscher sowie dubiose Entwickler an, die mit dem Verkauf von Exploits gutes Geld verdienen wollen. Einige davon finanzieren sich damit mittlerweile ihren Lebensunterhalt; und dies bisweilen auf gutem Niveau. Ein guter Exploit für Angreifer mit wirtschaftlichen Zielen kostet in der Regel 50 000 bis 250 000 USD. Browser-Exploits, populäre Betriebssysteme und Software-Komponenten stehen hoch im Kurs.

Neben einem Markt für Exploits werden aber ebenso die gestohlenen Daten gehandelt. Dass man im Darknet Kreditkarten, Kontodaten, Drogen und Waffen kaufen kann, ist altbekannt. Die starke Zunahme des Angebots von Patientendaten wird aber vor allem im Gesundheitsbereich mit Unbehagen beäugt. Generell werden punktuell Geschäftsgeheimnisse verkauft, die ihrerseits ein Problem für Industrie- und Technologieunternehmen darstellen. Die Preise varieren dabei sehr stark und sind schwierig generisch vorauszusagen. Aber auch da hat sich mittlerweile ein Markt etabliert, der dank erweiterter Angriffsflächen über Smartphones und IoT (Internet of Things) vorerst nicht austrocknen wird.

Attacken auf Spezialkomponenten

Dass Angriffe auf herkömmliche Computersysteme möglich sind, steht ausser Frage. Ausgeklügelte Malware nutzt zum Teil genau solche Schwachstellen, um ein System infizieren zu können. Dies ist



teilweise sogar ohne Zutun des Benutzers möglich und deshalb besonders perfid.

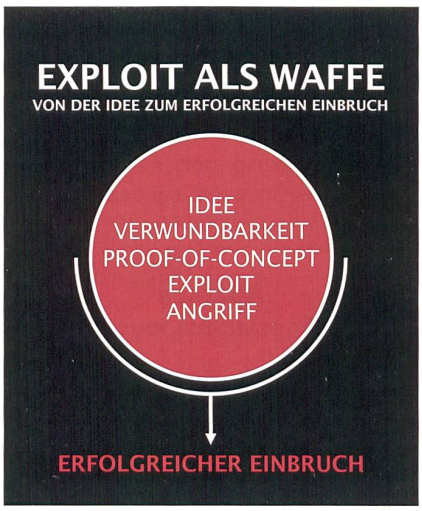
Dabei wird oftmals dem Irrglauben unterlegen, dass exotische Systeme und Spezialkomponenten gegen Angriffe geschützt sind. Zwei Gründe widerlegen dieses Ammenmärchen:

1) Es ist oft so, dass auch bei Spezialsystemen bekannte Mechanismen zum Einsatz kommen. Zum Beispiel werden viele Medizinalgeräte mit grundsätzlich herkömmlichen Windows- oder Linux-Systemen betrieben. Diese werden teilweise nur geringfügig modifiziert und grafisch anders aufbereitet.
2) Zudem ist eine gewisse Exotik nicht automatisch mit Sicherheit gleichzusetzen. Grundsätzlich finden sich in jedem Computersystem Schwachstellen, egal wie komplex oder unpopulär es sein mag. Überall wo Code ausgeführt wird, können Schwachstellen vorhanden sein und Malware-Infektionen durchgeführt werden.

In gewissen Bereichen ist man um eine möglichst sichere Entwicklung dieser Systeme bemüht. Dort werden dementsprechend erweiterte Mechanismen zur Validierung der Software eingesetzt. Dabei fokussiert man sich aber traditionellerweise auf die Funktionalität und Aspekte der «physischen Sicherheit» (auf Englisch hiesse es «safety» anstatt «security»).

Diese validierten und teilweise zertifizierten Systeme sind theoretisch robuster als herkömmliche Lösungen. Damit geht aber auch ein entscheidender sicherheitstechnischer Nachteil einher: Anpassungen und Optimierungen finden selten oder gar nie statt. Möchte man zum Beispiel bei einem zertifizierten System einen Fehler beheben, wird die erneute Zertifizierung erforderlich. Dies ist aufwendig und kostspielig, weshalb nach Möglichkeiten darauf verzichtet wird.

Dieselbe Trägheit kann dann auch im Betrieb beobachtet werden. Der Käufer des Produkts hat oftmals alle Hände voll damit zu tun, um dieses einsetzbar halten und einsetzen zu können. Für zusätzliche Anpassungen, wie das Einspielen von Security-Patches, bleibt dann oftmals keine Zeit. Das Resultat: Vielerorts werden veraltete und damit unsichere Spezialsysteme eingesetzt, die ein konkretes Risiko mit sich bringen. Je spezieller und exoti-



scher ein System ist, desto grösser ist dieses Risiko.

Gefahren des Cyberwar

Obwohl der Cyberspace laut NATO seit Mitte 2016 als Kriegsgebiet gilt (virtuelle Angriffe können den Bündnisfall auslösen), ist das Thema Cyberwar bis zum heutigen Tag umstritten. Es steht jedoch nicht zur Debatte, dass die moderne Kriegsführung von elektronischen und digitalen Komponenten abhängig ist. Und dass das Aushorchen und Manipulieren dieser dem Gegenüber einen entscheidenden Vorteil verschaffen kann.

Elektronische Systeme müssen deshalb mit Fokus auf die Sicherheit selber entwickelt werden, um ungewollten Einflüssen durch Dritte entgehen zu können. Niemand will eine Drohne oder eine Lenkwaffe kaufen, die im Einsatz dank einer Hintertür plötzlich durch den Feind übernommen werden kann.

Und falls sich Systeme aus technischen oder wirtschaftlichen Gründen nicht selber entwickeln lassen, müssen sie vor dem Kauf eingehend geprüft werden. Nur durch das Erzeugen von Transparenz können Überraschungen verhindert werden. Dies mag im Rahmen einer Anschaffung oder während der Vertragsverhandlungen unbequem erscheinen. Aber es ist erforderlich, denn sonst kauft man buchstäblich die teure Katze im Sack.

Gerade vernetzte Systeme müssen dementsprechend explizit geschützt werden. Geheimhaltung und Verstecken ist dabei kein echter Schutz. Im IT-Umfeld wird diese «Security by Obscurity» schon lange als naives Märchen entlarvt. Schutzmechanismen wie Verschlüsselung, Authentisierung und Segmentierung sind die einzig echten Mittel, um dem Ziel der Sicherheit einen Schritt näher kommen zu können. Nur so kann eine robuste Infrastruktur, auf die sich im Krisenfall verlassen werden kann, geschaffen werden.

Fazit

Cybersecurity ist ein Thema, das in den Mittelpunkt des alltäglichen Lebens vorrückt. Es betrifft uns alle, egal ob privat, beruflich oder in der Kaderfunktion in der Armee. Sich vor den Risiken zu verstecken, ist unmöglich, weshalb man sich mit ihnen auseinandersetzen muss.

Das grundlegende Verständnis für etablierte Mechanismen und Technologien ist dabei genauso wichtig, wie das Wissen um potentielle Bedrohungen. Es bleibt uns allen also nichts anderes übrig, als mit offenen Augen den digitalen Bereich im Blickfeld zu behalten.

Risiken können oftmals nicht komplett eliminiert werden. Manchmal muss man sie halt eingehen, das ist Teil des Lebens. Wenn man ein Risiko jedoch eingeht, muss man sich dessen bewusst sein und die Auswirkungen eines Eintretens in Kauf nehmen. Cybersecurity ist nicht einfach. Aber es liegt an jedem Einzelnen, es halt eben möglichst richtig zu machen. ■

Oberleutnant (Zivilschutz)
Marc Ruef
Head of Research
scip AG, Zürich
5436 Würenlos