SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

Juli 2016

SWITCH

I. DAO-ismus im ETHER-net: Ein Hacker erbeutet Kryptowährung im Wert von 50 Millionen US-Dollar

Vor Kurzem wurde bekannt, dass ein Angreifer eine offenbar schon länger bekannte Lücke in Form einer recursive calling vulnerability nutzte, um 3,6 Millionen ETHER-Tokens aus dem virtuellen Investmentfond DAO abzuzweigen, die zum Angriffszeitpunkt einen Wert von mehr als 50 Mio. USD darstellten – mehr als 35 Prozent des Fondsvermögens.

Um zu verstehen, warum daraus eine Kryptowährungskrise mit weiter reichenden Konsequenzen werden könnte als der Angriff auf Mt. Gox, in dessen Folge die bekannteste Börse für Bitcoins Insolvenz anmelden musste, ist es nötig, sich die einzelnen Bestandteile – DAO, die Blockchain Ethereum, die recursive vulnerability und die Optionen nach dem Hack – näher anzusehen.

DAO wurde als Alternative zur klassischen Risikokapitalgeber-Finanzierung entwickelt. Die Idee: An die Stelle einer von Menschen und deren des Öfteren vom Firmenziel abweichenden Einzelinteressen geführten Investmentfirma sollte ein dezentrales Netzwerk aus sich selbst ausführenden digitalen Verträgen (Smart Contracts) treten – die Decentralized Autonomous Organisation DAO war

geboren. Menschen tauchen nur noch auf, wenn sie Anteilseigner von DAO werden wollen. Dazu erwerben sie digitale Tokens – im Fall von DAO in ETHER, der Kryptowährung, die in der Blockchain Ethereum, einem dezentralisierten Peer-to-Peer-Netzwerk gehandelt wird. Die Zahl erworbener ETHER legt den Umfang der Stimmrechte fest, mit denen die Stimmrechtsinhaber in einer dem E-Voting vergleichbaren elektronischen Abstimmung wählen, wo und wie das Geld investiert werden soll. Im weiteren Unterschied zu einer traditionellen Investmentfirma hat DAO keine reale Adresse und ist damit – zumindest in der Theorie – für Staaten und deren Finanzregulatoren und Steuerbehörden ebensowenig antastbar wie für Aussenstehende. Die Ethereum-Blockchain-Struktur bringt DAO doppelt Vorteile: Anders als in der Bitcoin-Blockchain, können auf Ethereum komplexere Vorgänge, wie z.B. Programme oder eben Smart Contracts getauscht werden. Weil aber wie in jeder Blockchain auch Ethereum sicherstellen muss, dass Informationen jederzeit im Netzwerk gefunden werden können, lassen sich die dazu verwendeten Adress- und Buchstabencodes bestens als anonyme Nummernkonten verwenden.
Dass der DAO-Hack über eine «einfache» recursive calling vulnerability gelaufen ist, bringt DAO gleich in mehrere Erklärungsnöte. Zwar ist technisch transparent und bekannt, wohin die ETHER abgezogen wurden, aber niemand weiss, wem das Konto gehört, auch wenn auf pastebin.com ein anonymes Bekennerschreiben veröffentlicht wurde. Darin erklärt der vermeintliche Dieb, dass er nichts Unrechtes getan, sondern lediglich die Möglichkeiten des DAO-Codes genutzt habe.

Tatsächlich stellt die damit aufgeworfene Frage, ob die Ausnutzung eines Programmfehlers überhaupt als Hack oder als Verbrechen gewertet werden kann, wenn just jener Programmcode das bindende Element des Vertrags sein soll, das gesamte Konzept der Smart Contracts zur Diskussion – zumal die DAO-Entwickler sich inzwischen derselben Methodik bedient haben, um das verbliebene Kapital vor weiterem unberechtigtem Abzug zu schützen. Zudem hat der Angriff deutlich und laut gezeigt, dass die von DAO proklamierte Sicherheit und Unantastbarkeit doch nicht gewährleistet war. Zum anderen würden aber alle diskutierten Möglichkeiten, die Tokens (und damit das Geld) zurückzuholen, die Glaubwürdigkeit und das Vertrauen in DAO untergraben. Und schliesslich

zeigt sich, dass sich der vermeintliche Vorteil, keine reale Adresse zu haben, dann in einen Nachteil verwandelt, wenn reale Strafverfolgungsbehörden und Gerichtsbarkeiten gefordert wären, die aber für eine Firma, die ohne reale Adresse existiert ja bewusst ausgeschlossen waren.
Es bleibt abzuwarten, wie sich der Fall weiterentwickelt und wie er sich auf eine Motion auswirken wird, die am 16. Juni 2016 im Schweizer Nationalrat eingereicht wurde, um die Sicherheitsauflagen für Start-Ups zu lockern, die via Blockchains Finanzgeschäfte abwickeln wollen.

Nachzulesen unter:

http://www.zeit.de/digital/internet/2016-06/the-dao-blockchain-ether-hack/komplettansicht
http://www.wired.com/2016/06/50-million-hack-just-showed-dao-human
http://www.zeit.de/digital/internet/2016-05/blockchain-dao-crowdfunding-rekord-ethereum
https://de.wikipedia.org/wiki/Ethereum
http://www.btc-echo.de/dao-hack-falsche-entscheidung-ethereum-zerstoeren
http://www.zeit.de/digital/internet/2016-05/blockchain-dao-crowdfunding-rekord-ethereum
http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs
http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit
http://pastebin.com/CcGUBgDG
http://www.heise.de/newsticker/meldung/Nach-dem-DAO-Hack-Verbliebenes-Kryptogeld-mit-freundlichem-Hack-gesichert-3246539.html
http://www.computerworld.ch/news/it-branche/artikel/politiker-wollen-tiefere-huerden-fuer-blockchain-gruender-70394
http://www.digitale-nachhaltigkeit.ch/2016/06/blockchain-motion

II. Smart, gierig und nicht tot zu kriegen: Ransomware

Dass auch virtuelle Erpresser ermüden und aufgeben, zeigt das Ende von TeslaCrypt. Am 18. Mai berichtete bleeping computer, dass dessen Entwickler schon Wochen zuvor begonnen hatten, sich nach und nach zurückzuziehen. Überraschenderweise kamen sie auch der Bitte eines Sicherheitsexperten nach, den Masterkey zur kostenlosen Entschlüsselung ins Netz zu stellen, so dass alle Erpressten ihre Daten ohne Lösegeldzahlung aus ihrem virtuellen Gefängnis holen können (wie der Decoder zu verwenden ist, ist im Link zu Bleeping Computer unten detailliert beschrieben).

Wer dagegen die dreiwöchige Aktivitätspause, die der «Locky»-Erpressungstrojaner im Juni eingelegt hatte, als Zeichen der Hoffnung wertete, wurde ganz schnell in die Niederungen des Cybercrime zurückgeholt: Locky ist

wieder aktiv und scheint alles daranzusetzen, seinen fragwürdigen Ruf als «most dominant ransomware distributed in spam email» – so der Cybersecurity-Anbieter FireEye – weiter festigen zu wollen. So wütet der Erpressungstrojaner inzwischen wieder auf gleichem Aktivitätslevel wie zuvor. Pause haben seine Entwickler offenbar genutzt, um einen Ableger zu entwickeln, der sein schmutziges Geschäft nicht nur smarter beherrscht als Locky, sondern auch weit gieriger daherkommt. Zwar versucht auch «Bart», so der Name der Ransomware, Windows-User zum Öffnen eines eMail-Anhangs zu bewegen, um via RockLoader und HTTPS Malware auf den Rechner zu schleusen. Die verschlüsselt die Daten aber als passwortgeschützte ZIP-Dateien. Und zwar auch dann, wenn eine Firewall Verbindungen zwischen Malware und Command-and-Control-Server blockieren würde. Dafür verlangt Bart für das Entschlüsseln der gekidnappten Dateien nicht die «branchenüblichen» 0,5, sondern 3 Bitcoin, also statt ca. 300.- über 1.800 Franken!

Schlechte Nachrichten auch vom Cyberhöllenhund «Cerber»: Neuerdings nimmt der Verschlüsselungs- und Erpressungstrojaner nicht nur Daten in Geiselhaft, sondern missbraucht die geschädigten Rechner zusätzlich als Bots, um DDoS-Angriffe auf Ziele der Cyberkriminellen zu starten. Die Entdecker dieser unerfreulichen Tatsache stellen ihre Erkenntnisse unter den Titel: «Zwei Angriffe zum Preis von einem.» Es scheint so, als sei der Spar- und Effizienzzwang auch in der virtuellen Unterwelt angekommen.

Angekommen ist dort auch, dass «smart» ganz neue Möglichkeiten eröffnet. So treibt etwa FLocker seit April 2015 auf Android-Smartphones sein erpresserisches Unwesen. Eine Variante davon befällt jetzt auch Smart-TVs. Gemäss den Sicherheitsforschern von Trendmicro verschlüsselt der TV-FLocker aber keine Dateien, sondern sperrt den Bildschirm und zieht Daten aus den Geräten, sofern diese sich nicht in Armenien, Aserbaidschan, Bulgarien, Georgien, Kasachstan, der Ukraine, Ungarn oder Russland befinden (ob daraus Rückschlüsse auf die Domizilierung der Hintermänner gezogen werden können, ist derzeit nicht klar).

Nachzulesen unter:

https://www.switch.ch/news/ransomware-day
http://www.20min.ch/digital/news/story/27616624
http://www.economiesuisse.ch/de/artikel/das-bewusstsein-erhöhen-für-internet-gefahren
http://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key

http://www.heise.de/security/meldung/I-f-Sorry-Bitte-benutzen-Sie-dieses-kostenlose-Entschluesselungs-Tool-3217315.html
https://www.fireeye.com/blog/threat-research/2016/06/locky-is-back-and-asking-for-unpaid-debts.html
http://www.heise.de/security/meldung/Locky-Sproessling-Erpressungs-Trojaner-Bart-verschluesselt-anders-und-verlangt-hohes-Loesegeld-3250058.html
http://www.heise.de/security/meldung/Neben-Erpressung-nun-auch-DDoS-Verschluesselungs-Trojaner-Cerber-lernt-dazu-3217254.html
https://www.invincea.com/2016/05/two-attacks-for-the-price-of-one-weaponized-document-delivers-ransomware-and-potential-ddos-attack
http://www.zdnet.de/88272059/ransomware-flocker-legt-android-basierte-smart-tvs-lahm/

III. CANVAS in den Startlöchern: Wie gehen Ethik und Cybersecurity zusammen?

Je komplexer das digitale Ökosystem auf der einen und je grösser die globalen Risiken auf der anderen Seite werden, desto grösser wird die Gefahr, dass die Durchsetzung von Cybersicherheit andere fundamentale Werte wie Freiheit, Gleichheit, Fairness oder Privatsphäre in Mitleidenschaft ziehen könnte. Um dieser Gefahr zu begegnen, wird im September 2016 das CANVAS-Konsortium seine Arbeit aufnehmen. CANVAS steht für Constructing an Alliance for Value-driven Cybersecurity. Wissenschaftler, Praktiker und Datenschützer aus elf Institutionen in sieben europäischen Ländern sollen ein Netzwerk von IT-Entwicklern und Fachleuten aus Ethik, Recht und Sozialwissenschaften schaffen, um vor allem das Gesundheitssystem, das Finanzwesen sowie die Strafverfolgung bzw. nationale Sicherheit zu untersuchen. Ziel ist es, nach Bestandsaufnahme und Analyse geeignetes Briefing-Material für die Politik, aber auch einen Referenz-Studiengang für die Ethikausbildung von IT-Experten und ein MOOC (Massive Open Online Course) für werteorientierte Cybersecurity zu entwickeln.

Das Thema beschäftigt offenbar auch den US-amerikanischen Open Technology Fund, der die Arbeiten von Ben Zevenbergen vom Oxford Institute for the Internet an der University of Oxford fördert. Zevenbergen forscht als Jurist über Ethik in vernetzten Systemen und hat als Keynote-Speaker der Troopers 16 im März in Heidelberg in einem beachtenswerten Vortrag eine interessante These aufgestellt. Nach seinen Forschungsergebnissen arbeiten IT-Entwickler prioritär nach dem utilitaristischen Ansatz «Der Zweck heiligt die Mittel», und damit diametral entgegengesetzt der Denkweise der Sozial-, Geistes- und

Rechtswissenschaftler, für die generell gültige ethische Regeln auf allen Stufen eines Entwicklungsprozesses einzuhalten sind. In Zeiten der Digitalisierung aller Lebensbereiche bräuchte es nach seiner Meinung eine Symbiose beider Denkweisen. Sein Fazit: «Um die Welt zu einem sichereren Ort zu machen, braucht es nicht nur die Skills der IT-Entwickler, sondern auch ethische Grundlagen und Guidelines.»

Nachzulesen unter:

http://www.ethik.uzh.ch/de/ufsp/forschungsprojekte/nemos/forschungsprojekte/CANVAS.html
http://www.regensburg-digital.de/eine-bruecke-zwischen-cybersicherheit-und-ethik-das-canvas-konsortium/20052016
http://www.heise.de/security/meldung/Forschungsprojekt-Wie-gehen-Ethik-und-Cybersecurity-zusammen-3239827.html
https://www.researchgate.net/publication/289489876_Philosophy_Meets_Internet_Engineering_Ethics_in_Networked_Systems_Research
https://www.youtube.com/watch?v=9xEaokeP0mg

IV. Wenn der US-Grenzschutz Facebook-Freund werden will – und andere News zum Thema «Anti-Terror-Pakete»

Die US Customs and Border Protection genannte amerikanische Grenzschutzbehörde hat beantragt, die Einreiseformulare für Nicht-US-Bürger so zu verändern, dass diese ihre Social Media Accounts nebst Profilnamen dort eintragen können – vorerst zumindest noch freiwillig. Begründet wird der Schritt damit, dass die Behörde Einreisende damit besser erreichen kann. Hintergrund ist aber offenbar, dass man sich im Bedarfsfall leichtere Ermittlungen nach Anschlägen oder von Verbindungen zu Terrorgruppen erhofft. Es steht zu befürchten, dass jeder, der sich nicht ins amerikanische Sing-Sing zwitschern will, künftig vor seinem US-Aufenthalt deutlich zurückhaltender kommunizieren sollte als mancher Präsidentschaftskandidat.

Mit neuen Ideen will aber auch die deutsche Bundesregierung Licht ins digitale Dunkel bringen, das sich aus ihrer Sicht durch die anbieterseitige Verschlüsselung z.B. von WhatsApp-Nachrichten oder iPhone-Sperrcodes ausbreitet. Nach ihrem Willen sollen bald 400 Menschen in einer neuen Sicherheitsbehörde namens Zitis daran arbeiten, Entschlüsselungstechniken zu entwickeln, damit Polizei, Verfassungsschutz und Kriminalämter trotz

anbieterseitiger Verschlüsselung die Internetkommunikation Verdächtiger mithören und -lesen können. Die in Deutschland gebotene Trennung zwischen Polizei und Geheimdienst ist nach Meinung von Bundesinnenminister de Maiziére deshalb nicht beeinträchtigt, weil Zitis nicht selbst Daten sammle, sondern nur die dafür nötigen Techniken entwickeln oder zukaufen soll. Der frühere Bundesbeauftrage für den Datenschutz, Peter Schaar, nahm die Ankündigung der neuen Behörde zum Anlass, darauf hinzuweisen, dass die Aufrüstung der Dienste immer stärker forciert werde, dieser Effort aber bei den Aufwändungen für den Datenschutz nicht zu erkennen sei. CANVAS (siehe Thema III) startet offenbar nicht zu früh.

Nachzulesen unter:

http://www.theverge.com/2016/6/24/12026364/us-customs-border-patrol-online-account-twitter-facebook-instagram
https://www.wired.de/collection/life/bei-der-usa-einreise-koennten-bald-eure-social-media-profile-abgefragt-werden
http://www.computerworld.ch/news/it-branche/artikel/us-einreisebehoerden-wollen-zugriff-auf-social-media-accounts-70420
http://www.heise.de/security/meldung/Datenschuetzer-Peter-Schaar-kritisiert-Plaene-fuer-neue-Sicherheitsbehoerde-3249124.html

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.