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

November/Dezember 2019

I. Innere Sicherheit – ein Thema nicht nur für Sicherheitsfirmen

Security-Firmen gelten als starke Verbündete der Userinnen und User im Kampf gegen Hacker, Spammer und andere Cyberkriminelle. So vertrauen z.B. mehr als 12 Millionen Kunden weltweit auf Cybersicherheitsprodukte des japanischen Unternehmens Trend Micro. Dieses wurde im August 2019 selber Opfer eines Cyberangriffs – und zwar von innen. Anfang November berichtete threatpost, dass sich ein "rogue employee", also ein Mitarbeiter unberechtigten Zugang zu einer Datenbank verschafft hatte und von dort Namen, E-Mail-Adressen, Support-Ticket-Nummern und in verschiedenen Fällen die Telefonnummern von 68.000 Kunden gestohlen und weiterverkauft hatte. Die Opfer dieses Datenlecks wurden kurz darauf telefonisch von Betrügern kontaktiert, die sich als Trend Micro-Support-Mitarbeiter ausgaben. Einige der angerufenen Kunden kontaktierten das Unternehmen, das daraufhin eine Untersuchung einleitete und Anfang November den Datendiebstahl bestätigte, ohne näher bekanntgeben zu können, wer die Daten gekauft hatte.

Kundendaten von Sicherheitsfirmen sind wie die von Internet- und Social Media-Plattformen überaus wertvoll und eine «Goldgrube» für interne Kriminelle. So berichtet threatpost im gleichen Post, dass auch Snap und Facebook Probleme mit Mitarbeitern hatten, die ihren Zugang zu Kundendaten missbraucht hatten. Der Verizon Data Breach Investigations Report 2019 schätzt, dass Insider Threats für fast einen Drittel aller Datenlecks verantwortlich sind.

Umso unverständlicher wird angesichts dieser Bedrohungslage, wie leichtfertig (um nicht zu sagen: schlampig) manche Unternehmen mit den Daten ihrer Kunden umgehen. So hat die auf die Vermittlung von Geschäftsreisen spezialisierte Hotelbuchungsplattform der französischen Gekko Group in einer ungeschützten und unverschlüsselten Elasticsearch-Datenbank einen mehr als ein Terabyte grossen Datensatz mit Buchungsinformationen, Kreditkartendetails sowie Zugangsdaten von Kunden der AccorHotels und verschiedener Subunternehmen, vor allem Teldar Travels und Infinite Hotels abgelegt. Gekko hat nach eigenen Angaben den Server gesichert, steht aber mit seinem schluderig-riskanten Umgang mit Kundendaten nicht alleine da: Im Oktober waren knapp 7,5 Millionen Kundenkonten der Adobe Creative Cloud ebenfalls in einer offenen Elasticsearch-Datenbank ungeschützt im Netz einsehbar.

Und auch Wizards of the Coast – Entwickler des beliebten Sammelkartenspiels "Magic - The Gathering" lagerte ein Datenbank-Backup ungeschützt und frei zugänglich in der Cloud – mit mehr als 452.000 Benutzerkonten des Online-Spiels samt E-Mail-Adressen und gehashten Passwörtern. Gemäss eigenen Angaben wollte das Unternehmen die betroffenen Spieler informieren und sie auffordern ihr Passwort zu ändern. Und weil der Brexit immer noch nicht vollzogen ist, zeichnet sich hier auch ein grösserer meldepflichtiger und sanktionsbedrohter Vorfall im Rahmen der Europäischen Datenschutzgrundverordnung ab.

Dass trotz aller Vorsichtsmassnahmen gezielte Angriffe von aussen immens erfolgreich sein können, musste der Elektronik-Versandhändler Conrad Electronic im November erfahren. Da war aufgefallen, dass unbekannte Angreifer eine Sicherheitslücke in der Elasticsearch-Datenbank das Multi-Channel-Händlers über Monate hinweg dazu genutzt hatten, nahezu 14 Millionen Kundendatensätze abzusaugen. Zwar seien weder Kreditkarteninfos noch Kundenpasswörter abgeflossen, doch hätten die Hacker Post- und E-Mail-Adressen, Fax- und Telefondaten und in etwa 280.000 Fällen die IBAN-Nummern gestohlen.

Auch im Conrad-Fall wurde die Sicherheitslücke geschlossen. Der Unternehmensinhaber entschuldigte sich bei den Kunden und informiert darüber, dass er Strafanzeige erstattet und die Datenschutzbehörden gemäss DSGVO verständigt habe.

Nachzulesen unter:

https://threatpost.com/trend-micro-rogue-employee-68k-customers/149946
https://threatpost.com/verizon-dbir-espionage-c-suite-cloud/144486
https://www.heise.de/newsticker/meldung/Datenleck-Kundendaten-von-Hotelbuchungsplattform-ungeschuetzt-im-Internet-4592945.html
https://techcrunch.com/2019/11/16/magic-the-gathering-wizards-data-exposure
https://www.heise.de/newsticker/meldung/Unbekannte-dringen-in-Server-von-Conrad-Electronic-ein-4591326.html

II. CNAME-Cloaking – der neue Angriff auf die Privatshpäre

Spätestens seit er in Verbindung mit dem Cambridge Analytical-Skandal im Umfeld der letzten US-Präsidentschaftswahl gebracht wurde, gilt Michal Kosinski vielen Kritikern als Totengräber der Privatsphäre. Schliesslich fordert er u.a. in einem Interview mit der NZZ, dass wir uns von ihr verabschieden sollten, um zum einen die positiven Outcomes der Digitalisierung besser nutzen zu können. Aber auch, um uns zum anderen unvoreingenommener mit der in seinen Augen weit grösseren Bedrohung durch KI auseinandersetzen zu können.

Mit seiner Forderung dürfte der heute in Standford lehrende Professor der Psychometrie Wasser auf die Mühlen der "Tracking-Gammel-Buden" (Zitat: Mike, Kuketz, kuketz-blog.de, Verlinkung unten) giessen, die mit CNAME-Cloaking einen neuen Weg gefunden haben, uns zu tracken und Werbung an Werbeblockern vorbeizuschleusen. Denn trotz aller Adblocker und Add-Ons für Internet- und Mobile-Browser sind Online-Werber hinter den Daten und der Aufmerksamkeit von Usern her wie die Orks hinter der Gemeinschaft des Rings in den Minen von Moria. Und deshalb suchen sie nach immer neuen Wegen, immer raffinierter Adblocker und Add-Ons auszutricksen. Nun scheinen Werbefirmen wie z.B. Eulerian, die neben Warner Brothers auch grosse französische Marken von Canal+ bis zu den F. Leclerc Supermärkten als Referenzen nennen, in CNAME-Cloaking einen Weg gefunden zu haben, der nahezu alle gängigen Anti-Tracking-Anstrengungen austrickst.

Dabei steht CNAME für Canonical Name und Cloaking für Tarnung – angesichts dessen bleibt die Frage, ob es arroganter Zynismus oder völliger Realitätsverlust ist, wenn Eulerian auf der eigenen Website "Transparenz" als einen von vier Firmenwerten aufführt. Denn die Bezeichnung ist Programm: Zwar schützen gängige Adblocker oder eingebaute Tracking-Schutzroutinen vor bekannten Werbe- und Tracking-Domains. Jedoch eben nur vor diesen. Wenn sie nun aber immer wieder unter neuen, zufällig im Domain Name System DNS generierten Namen daherkommen, hat der Antitracker keine Chance, diese als jene Werbewebsite zu erkennen, die er eigentlich blocken soll. Derzeit ist einzig das momentan auch nur in Beta-Version verfügbare uBlock origin-Add On für Firefox ab

Version 60 in der Lage, Tracking unter Einsatz von CNAME-Cloaking zu unterbinden. So jedenfalls die Einschätzung von Mike Kuketz, Security-Blogger, Penetrationstester und Mitarbeiter des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg. uBlock origin nutzt dabei eine Programmierschnittstelle, die Hostnamen eines DNS-Eintrags auflösen und damit den eigentlichen Absender enttarnen kann. Googles Chrome und Apples Safari haben keine vergleichbare Schnittstelle und können daher CNAME-Tracker nicht enttarnen. Bei Chrome scheint dies auch gar nicht mehr gewollt zu sein. Denn das Google "Manifest v3" sieht vor, dass AddOns zu Chrome Browseranfragen künftig nur noch lesen, nicht aber verändern oder gar blockieren können.

Nachzulesen unter:

https://www.nzz.ch/feuilleton/michal-kosinski-facebook-ist-phantastisch-fuer-die-demokratie-ld.1520699
https://www.heise.de/newsticker/meldung/Firefox-uBlock-Origin-schuetzt-vor-versteckten-Trackern-4596641.html
https://tarnkappe.info/cname-cloaking-neue-tracking-methode-trickst-adblocker-aus
https://medium.com/nextdns/cname-cloaking-the-dangerous-disguise-of-third-party-trackers-195205dc522a
https://www.theregister.co.uk/2019/11/21/ublock_origin_firefox_unblockable_tracker

III. Verheerender Malware-Cocktail – Emotet & Co. Und ganz neu: NextCry für Linux

Bereits im letzten SWITCH Security-Report hatten wir – da schon zum zweiten Mal in diesem Jahr – auf die immensen Schäden hingewiesen, welche die Ransomware der Emotet-Gruppe flächendeckend anrichtet. Dass wir nun in kurzem Abstand zum dritten Mal vor Ransomware warnen, liegt daran, dass die im letzten Report (und im ersten heise.de-Link unten nochmals ausführlich) beschriebene Angriffskaskade nach wie vor aktiv und immer noch brandgefährlich ist. In Kurzform: Personalisierte Spam-Mails exponierter Vertreter von Unternehmen oder Organisationen fordern dort Mitarbeitende zum Öffnen eines infizierten Word-Anhangs auf, mit dem Emotet auf die Windows-Rechner der Mitarbeitenden gelangt und damit die initiale Komprommitierung darstellt. Dann wird TrickBot nachgeladen, um Zugangsdaten zu Konten abzuphishen, sich lateral auf den Systemen des Opfers weiterbewegen zu können, und um beispielsweise zu verstehen, wie die Datensicherungssysteme funktionieren. In der dritten Stufe wird der Verschlüsselungstrojaner Ryuk nachgeladen, der sich dank integrierter Wurm-Komponente durch das gesamte Netzwerk fressen und dort sämtliche Daten verschlüsseln kann. Diesen Cocktail bezeichnen CERTs und IT-Sicherheits-Organisationen bisweilen als eines der zerstörerischsten und kostenträchtigsten Angriffe überhaupt.

Jüngstes Opfer wurde der global agierende spanische Sicherheitsdienst Prosegur, dessen

175.000 Mitarbeiter in 25 Ländern Personenschutz, Sicherheitsdienste, Geld- und Werttransporte sowie die Planung, Installation und Wartung von Gefahrenmeldeanlagen erbringen. Ende November meldete Prosegur einen Emotet-TrickBot-Ryuk-Angriff, der das Unternehmen in seinen Funktionen streckenweise zum Erliegen gebracht hatte. Gute 24 Stunden später gab das Unternehmen bekannt, Ryuk identifiziert und gebannt zu haben, dennoch waren nicht alle Dienstleistungen in vollem Umfang verfügbar.

Während Emotet und Co. in der Windows-Welt wüten, muss auch die Linux-Welt aufschreien: Denn dort treibt seit Mitte November "Nextcry" sein erpresserisches Unwesen. Das meldete Mitte November die Sicherheits-Website bleepingcomputer.com. Offenbar hatten die Angreifer eine inzwischen gepatchte Sicherheitslücke im FastCGI-Prozessmanager PHP-FPM (CVE-2019-11043) von Nextcloud-Servern mit NGINX als Reverse-Proxy genutzt, um die gespeicherten Daten so zu verschlüsseln, dass sie ohne Lösegeldzahlung nicht mehr entschlüsselt werden können. Im eigenen Blog verweist Nextcloud auf Sicherheitsupdates und darauf, dass 2 von 300.000 Nexcloudservern gehackt worden seien, ohne dass Lösegeld gezahlt worden wäre. Zugleich bekräftigt der Anbieter, dass man der Stellenwert von IT-Security gar nicht hoch genug einzuschätzen sei. Angesichts der Schäden, die Ransomware verursacht, ist dem nichts hinzuzufügen.

Nachzulesen unter:

https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html
https://www.zdnet.com/article/security-firm-prosegur-weve-shut-our-it-network-after-ryuk-ransomware-attack
https://www.heise.de/newsticker/meldung/Sicherheitsvorfall-beim-Sicherheitsdienst-Ransomware-Ryuk-befaellt-Prosegur-4598361.html
https://www.bleepingcomputer.com/news/security/new-nextcry-ransomware-encrypts-data-on-nextcloud-linux-servers
https://www.heise.de/security/meldung/Ransomware-NextCry-greift-Nextcloud-Server-an-4588421.html
https://nextcloud.com/blog/nextcry-or-how-a-hacker-tried-to-exploit-a-nginx-issue-with-2-nextcloud-servers-out-of-300-000-hit-and-no-payout

IV. Account-Löschungen und Fake-News-Bekämpfung auf Social Media Plattformen sorgen für Ärger

Twitter und Instagram wollen neu inaktive Accounts löschen, ernten dafür aber teilweise wüste Proteste der Account-Inhaber. Während Twitters Ankündigung, inaktive Accounts zu löschen, um "akkuratere, glaubwürdigere Informationen" zu "verbreiten, denen Leute auf Twitter vertrauen können", weitgehend ohne Reaktionen seitens der Userinnen und User blieb, protestierte die Adult Performers Actors Guild APAG, dagegen, dass Instagram mehr als 1.000 Accounts seiner Mitglieder gelöscht habe, weil sie nach Meinung Instagrams die Community-Regeln verletzt hätten. Die Protestierenden warfen der Social Media-Plattform Doppelmoral vor, weil sie vielfach überhaupt kein Problem damit habe,

frauenfeindliche Inhalte zu veröffentlichen. Grundsätzlich sehen die Instagram-Regeln vor, dass Nacktheit weder auf Fotos, Videos noch in anderen digitalen Inhalten publiziert werden dürfe. Dennoch gelten diese Regeln offensichtlich nicht in gleichem Mass für alle Userinnen und User.

Inkonsequenz und Widersprüchlichkeiten bei der Anwendung von Richtlinien zur (Nicht-) Veröffentlichung von Inhalten führen auch bei anderen Social Media-Plattformen immer wieder zu Diskussionen. So bezweifelt z.B. Donna Lu in einem Artikel auf newscientist.com, dass Facebooks Bemühen, Fake News einzudämmen, indem u.a. auch Fake Accounts gelöscht werden, von Erfolg gekrönt sein könnte. Zur Begründung verweist sie darauf, dass der Social Media Riese seine unter dem Eindruck des Nachhalls des Cambridge-Analytica-Skandals und der Rufe nach Facebooks Zerschlagung streng formulierten Werberichtlinien im Oktober still und heimlich wieder deutlich abgeschwächt worden waren. Zudem stellt sie die Frage, wie die beiden Monitoring Partner, die Facebook vor den britischen Parlamentswahlen einsetzen will, die Milliarde täglicher Posts sichten will, wenn der grössere der beiden Partner weniger als zehn Menschen damit beschäftigt.

Und Unternehmen, die bisher via WhatsApp Newsletter an Tausende von Abonnenten verschickt hatten, sind ratlos und – um höflich zu bleiben – sauer auf den zum Facebook-Imperium gehörenden Messengerdienst, weil der ab 7. Dezember 2019 den Versand dieser Newsletter definitiv unterbindet und mit juristischen Massnahmen ahnden will, die mit der Sperrung des Accounts beginnen und kostenpflichtige Abmahnungen nach sich ziehen werden. Pikant dabei ist, dass der Newsletterversand schon immer gegen WhatsApps Geschäftsbedingungen verstossen hatte.

Nachzulesen unter:

https://futurezone.at/digital-life/twitter-loescht-profile-die-ein-halbes-jahr-inaktiv-sind/400687487
https://futurezone.at/digital-life/accounts-geloescht-pornostars-beschweren-sich-ueber-instagram/400687316
https://www.newscientist.com/article/2221963-facebook-has-a-plan-to-tackle-fake-news-heres-why-it-wont-work
https://www.internetworld.de/online-marketing/whatsapp/whatsapp-newsletter-firmen-7-dezember-tun-1727506.html

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