Cyber & Risk Trends

Cyber & Risk Trends im August 2020: „Canceling Culture“ und chinesische Hacker benötigen auch Einschulungen

EDITORIAL

Unsere Ableitungen der Cyber & Risk Trends entstehen durch eine kontinuierliche Beobachtung öffentlicher Quellen im Internet. Zu diesen Quellen gehören beispielsweise Web-Blogs bekannter Sicherheitsforscher, Meldungen von Aktivisten/Whistleblowern in sozialen Medien, Publikationen von universitären Einrichtungen, Analysen und technische Indikatoren von Sicherheitsfirmen sowie Expertenmeinungen zu geostrategischen Themen. Der Beobachtungszeitraum für diesen Bericht war Mitte Juli bis Mitte August 2020.

- **Politischer Aktivismus** entwickelt sich während der Corona-Pandemie aufgrund der gesellschaftlichen Auswirkungen, rasant weiter. Statt kompromittierendem Material über eine Person sind es nun öffentliche Aussagen die zu einem digitalen „Flashmob“ führen. **„Canceling Culture“** ist der Versuch von Randgruppen über Soziale- und Online-Medien, eine Person hinter ihrer Aussage als Täter/in darzustellen und mit dem beruflichen Ende der Karriere zu bestrafen, also dem „Canceling“. Opfer sind meist Personen, die ihren Unmut über gesellschaftliche Entwicklungen kundtun und dafür Humor oder humorvolle Umschreibungen anwenden. Was früher falsch, peinlich oder sarkastisch gemeint war, ist somit ein garantiertes Karriereende, wie diverse Randgruppen durch eine bewusste Politisierung von bestehenden Weltbildern befinden. Bekanntes Beispiel dafür ist der liberale Sprachphilosoph Noam Chomsky, der für viele zusammenfassend nur mehr als Holocaustleugner gilt, obwohl er Generationen von Kriegs- und Globalisierungsgegnern geprägt hat. Anschuldigungen gegen vermeintliche Täter werden sprachlich neutral in Begriffen wie „deeply unpleasant people“ verpackt. Vereinzelt sind bereits Europäer betroffen, sofern sie international im Rampenlicht stehen, wie etwa die Buchautorin J.K. Rowling. Dank Smart-Phone, Online-Streaming und Video-Beiträgen in sozialen Netzwerken können solche Vorfälle dokumentiert und rasch verbreitet werden. Online-Medien wie Tageszeitungen spielen bei „Canceling“ keine unwesentliche Rolle, weil die Vorverurteilung einer Person meist ohne Folgen bleibt, aber definitiv die Reichweite erhöht. Der Autor Daniel Kehlmann nennt diese Form des digitalen Rufmordes eine „amerikanische Selbstzerfleischung“ und sieht die Auslöser dafür im politischen Klima, einem fehlenden gesetzlichen Kündigungsschutz bzw. einer einseitigen Medienberichterstattung. Dieser Trend steht erst am Anfang und könnte bei uns vor allem Funktionsträger von großen internationalen Unternehmen bei öffentlichen Auftritten treffen.

- **Staatlich sanktionierte Spionage und Cyber-Kriminalität** zur Erpressung verschmelzen weiterhin: Wie Intel 471 aktuell berichtet, entwickeln sich Kriminelle über die Jahre hinweg zu politisch-sanktionierten Hackern, die dem Staat (Regime) zuarbeiten. Die beiden chinesischen Hacker Li Xiaoyu & Dong Jiazhi wurden beispielsweise 2015 in einem Forum beobachtet, wie sie um eine technische Erklärung für Software-Code einer Schadsoftware anfragten. Aktuell werden sie von der amerikanischen Justiz gesucht. In China, Russland und dem Iran werden seit einiger Zeit diverse Hacker-Gruppierungen beobachtet, die ihr Spektrum von krimineller Erpressung bzw. Bereicherung durch Diebstahl digitaler Ressourcen auf staatlich-sanktionierte Spionage erweitern. Weitere Beispiele dafür sind die Evil Corp. in Russland, das Mabna Institute im Iran bzw. die ehemalige chinesische Sicherheitsfirma Boyusec (博御信息). [Danke an Intel 471 für die fachliche Unterstützung.]

- **Geopolitisch** entwickelt Nordkorea seine eigene Software für Cyber-Kriminalität weiter. Grundlage dafür ist das technische Unterfangen, die Schadsoftware „VHD“ über alle Betriebssystem-Plattformen (Linux, MacOS, Windows) zu verteilen, zu spionieren und Unternehmen durch Datendiebstahl und Verschlüsselung von Dateien zu schädigen. Sicherheitsforscher sehen dieses Unterfangen skeptisch, da

auch legitime Softwarefirmen regelmäßig an solchen Software-Projekten scheitern. Das „Multi-Platform Targeted Malware Framework“ (kurz: „MATA“) entspricht exakt der aktuellen Denkweise des Regimes, im Rahmen derer Projekte in Komplexität und Größe alles Bisherige übertrumpfen müssen. So wird in der Hauptstadt Pyongyang ein neues Mega-Zentralspital gebaut, die dafür notwendigen grundlegenden Verbrauchsmaterialen fehlen und müssen über gemeinnützige Organisationen beschafft/erbettelt werden. In China gehen Huawei langsam die 5G-Chips für hochwertige Smart-Phones aus. Apple wird vermutlich mittelfristig seine Stellung im chinesischen Markt verlieren, da der US-Präsident per Dekret jede US-Zusammenarbeit mit den Betreiberfirmen von „WeChat“ bzw. „TikTok“ untersagt. Die Vorboten einer neuen geopolitischen Ordnung kommen dabei langsam an das Tageslicht: Eine „Canzuk Union“, bestehend aus Kanada, Neuseeland, Australien und UK, könnte als neuer Gegenpol zu China und den USA bald realistisch werden, findet der Historiker Andrew Roberts und zeigt erste Beispiele auf. Die nächste große Unbekannte wird, wie Donald Trump bei einer möglichen Wahlniederlage im November 2020 reagieren würde. Auch hier sind sich amerikanische Juristen noch uneins, wie dies rechtlich ausgehen könnte. Bevor es aber so weit kommen könnte, werden bewaffnete Bürgermilizen, die virtuelle Bewegung „QAnon“ und das kontinuierliche „Defunding“ der amerikanischen Post für ein gehöriges Chaos bei der kommenden Präsidentschaftswahl sorgen.

- Virtuelle Lösegelderpressungen werden während der Pandemie durch Betrugsmethoden wie dem „**Bitcoin Giveaway Scam**“ ergänzt. Mit einer schlichten Betrugsmasche werden die Opfer manipuliert: Wer innerhalb der nächsten 30 Minuten auf eine bestimmte Bitcoin-Adresse einen Betrag in Bitcoin schickt, bekommt diesen wahlweise von Bill Gates, Elon Musk, Steve Wozniak, Tim Cook, oder anderen „wohltätigen“ Personen verdoppelt. Für viele klingt das einfach zu verlockend, um betrügerisch zu sein. Der „Bitcoin Giveaway Scam“ wird über soziale Netzwerke wie Facebook, Twitter und YouTube viral verbreitet, deren Betreiberfirmen eine Weiterverbreitung technisch nicht unterbinden können oder wegen Werbeeinnahmen nicht unterbinden wollen. Der ehemalige Apple-Mitbegründer Steve Wozniak hat genau deswegen eine Klage gegen die Google-Tochter YouTube eingebracht. In diesem Zusammenhang wurde bei Twitter aufgedeckt, dass ein wichtiges und sensitives Administrations-Werkzeug, über 1.000 internen und externen Mitarbeitern zur Verfügung stand und so jugendliche Hacker den Zugang über Bestechung einfach erlangen konnten. Mit dem Werkzeug konnte der „Bitcoin Giveaway Scam“ über zertifizierte Benutzerkonten automatisiert verbreitet und umgesetzt werden.

Das nächste Update folgt im September. Haben Sie noch Fragen? Benötigen Sie Literaturhinweise zu den Beispielen oder interessieren Sie sich für unsere Leistungen in diesem Bereich? Unsere Spezialisten Ewald Kager und Lorenz Szabo stehen Ihnen gerne mit Rat und Tat zur Seite.

ANSPRECHPARTNER

Ewald Kager

Ewald.Kager@bdo.at
+43 732 272975 211

Lorenz Szabo

Lorenz.Szabo@bdo.at
+43 1 537 37 836