Cyber & Risk Trends

Nordkorea stiehlt unsere Kreditkarten im Netz und im Iran gab es möglicherweise einen Stuxnet 2.0-Angriff

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 Juni bis Mitte Juli 2020.

- Politischer Aktivismus ist während der Corona-Pandemie weiterhin bestimmendes Thema und **soziale Netzwerke** multiplizieren dies. Beispielsweise werden politisierte Vorfälle zur Maskenpflicht in sozialen Netzwerken viral verbreitet, um so vor systematischer Diskriminierung indigener Volksgruppen bzw. Minderheiten als die eigentlichen Opfer dieser Pandemie abzulenken. Bei Facebook wurden Anfang Juli Details zu einem internen Prüfbericht über Bürgerrechte im sozialen Netzwerk publik, wonach Facebook die virtuellen Hassreden nur schwer bis gar nicht kontrollieren kann. Der Bericht deckt einen Zeitraum von zwei Jahren ab und zeigt Probleme wie Wahlmanipulationen bzw. Weiterverbreitung von Falschnachrichten auf. Der Hauptgrund der aufgezeigten Probleme liegt, wie sooft beim Geschäftsmodell von Facebook, in den grundlegenden Software-Algorithmen des sozialen Netzwerks.

- Gezielte Industriespionage gleitet im Juli wieder in **staatlich sanktionierte Spionage** ab. So überlegt die US-amerikanische Justiz, das chinesische soziale Netzwerk TikTok in den USA komplett zu verbieten, da die Anwendung zuletzt ohne Zustimmung der Anwender den Inhalt der Zwischenablage kopierte und an Server weiterleitete. (TikTok ist die internationale Variante der chinesischen Plattform Douyin.) Wiederholt missbraucht TikTok das Vertrauen seiner meist jungen Benutzer, aber auch deren Eltern, und spioniert wahllos auf Smartphones. Aber auch iOS-Anwendungen wie LinkedIn oder New York Times machen solche unerwünschten Datenübertragungen der Zwischenablage, wie die neueste Beta-Version von Apples mobilen Betriebssystem iOS als Sicherheitswarnhinweis anzeigt. Was früher als Key-Logger-Computervirus bezeichnet wurde, ist heute eine „Datenanalyse für Betrugsprävention“ oder für eine „Produktverbesserung“. Oft enden diese Datenanalysen als Datenleck offen im Internet oder Mitarbeiterinnen und Mitarbeiter („Insider“) benutzen solche Daten für betrügerische bzw. kriminelle Handlungen. Ein Yahoo-Mitarbeiter suchte beispielsweise über Monate hinweg explizite Bilder in über 6.000 Yahoo-Benutzerkonten, knackte weitere Benutzerkonten seiner Opfer und kam statt der geforderten Gefängnisstrafe mit Hausarrest und Geldstrafe davon.

- Geopolitisch stehen **Iran, Nordkorea und Russland** im Juli wieder im Fokus. Im Iran brannte Anfang Juli ein „kleines Lager“ - später wurde der Brand als Explosion in einer atomaren Anreicherungsanlage bestätigt. Experten vermuten einen Cyberangriff, ähnlich dem Stuxnet-Angriff auf die Uranzentrifugen im Jahr 2010. Nordkorea ist vermutlich das einzige Land, das staatlich sanktionierte Cyberspionage zur Devisenbeschaffung einsetzen muss und verwendet aktuell die MageCart-Angriffstechnik, um Webseiten für Online-Shopping zum Diebstahl von Kreditkartendaten zu manipulieren. Eine Sicherheitsfirma bringt Beispiele und zeigt, welche Firmen hier die Geldwäsche für das Regime betreiben. Nach Cyberkriminellen in Nigeria haben sich auch russische Kriminelle auf den hoch-profitablen Betrug mit „Business E-mail Compromise“ (CFO Fraud) spezialisiert. Die Opfer werden gezielt im Bereich Mergers & Akquisition kontaktiert und dabei zur Überweisung hoher Geldsummen überredet.

- **Virtuelle Lösegelderpressungen** nehmen weiterhin rasant zu. Im Juni wurden diverse Logistikfirmen mit Datenlecks erpresst und im Juli fokussiert die neue Schadsoftware EKANS industrielle Kontrollsysteme – eine Kategorie des sogenannten „Internet of Things“. EKANS ist eine Ableitung der Schadsoftware SNAKE und demonstriert, wie rasant Schadsoftware abgeändert und adaptiert wird. Zum Internet of Things gehören auch Internet-Router, also die Hardware für unseren Internetzugang zu Hause. Die CISA, die amerikanische Bundesbehörde für Cybersicherheit, hat in diesem Zusammenhang eine Warnung bei Geräten der Firma Netgear ausgesprochen. Der ehemalige Cyberkriminelle Brett Johnson, heute Trainer für Unternehmen und Behörden, gibt in einem aktuellen Interview zu bedenken, dass viele Unternehmen ihre Mitarbeiterinnen und Mitarbeiter zwar auf die Sicherheit am Arbeitsplatz trainieren, die Cybersicherheit bei der Heimarbeit (im Home Office) während der Corona-Pandemie komplett vernachlässigt wird.

Das nächste Update folgt im August. 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