MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE JANUAR 2024
GEOPOLITIK IM CYBERRAUM & BURP BAMBDAS

GEOPOLITIK IM CYBERRAUM

Geopolitische Faktoren spielen eine nicht zu unterschätzende Rolle im Cyberraum. Welche Ziele verfolgt dabei China, und wie wirken sich diese auf die Welt aus?

BURP BAMBDAS & BCHECK IM FOKUS

Wir zeigen auf, wie die neuen Features Burp Bambdas und Bcheck innerhalb der Burp Suite für Web App Pentests verwendet werden können.

Januar 2024: Das läuft im neuen Jahr

Wie Sie sich bestens erinnern können, haben wir von der scip AG in der Dezember-Ausgabe unseres Newsletters einen kleinen Jahresausblick gewagt und einige Themen herausgepickt, die uns 2024 beschäftigen werden. Neben unserem Cybersecurity Forecast haben wir auch mal geschaut, was sonst noch so im neuen Jahr ansteht.

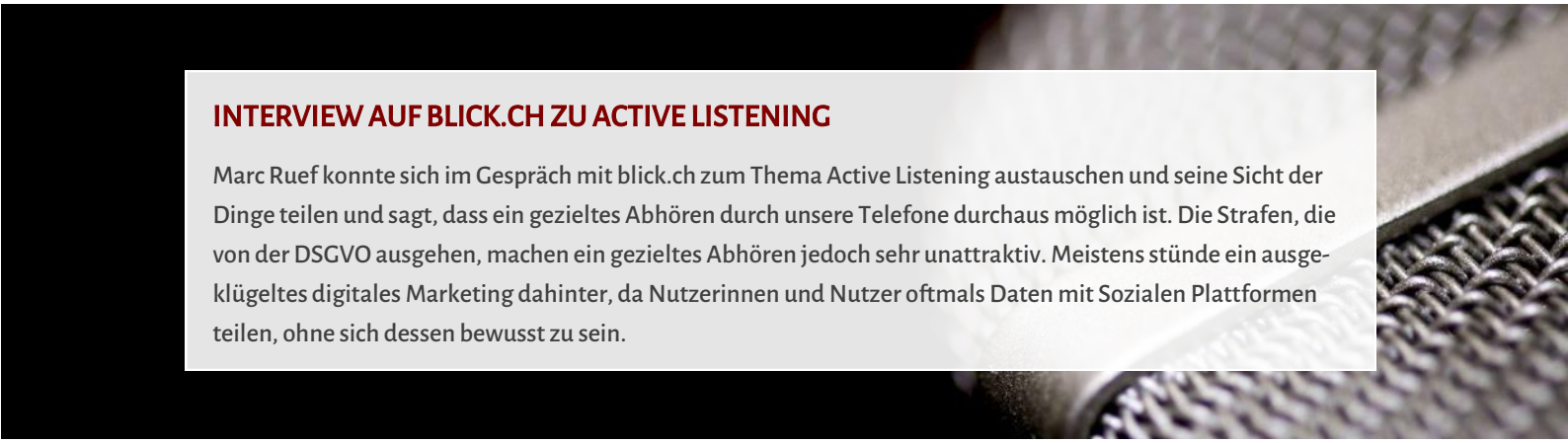
Rein sportlich gesehen ist 2024 ein ziemlicher Knüller: Mit der Fussball EM in Deutschland und den Olympischen Spielen in Paris wird der Sommer bestimmt nicht langweilig. Darüber hinaus hosten wir als Gastgeberland die Rad Weltmeisterschaft in Zürich, welche im September stattfinden wird. Auch politisch gesehen stehen im 2024 entscheidende Wahlen an: Gerade erst hat Taiwan sein neues Parlament und seinen demokratisch-progressiven Präsidenten William Lai gewählt. Putin tritt im Frühling erneut für Russland an, und in der Türkei, Indien oder Indonesien stehen ebenso Präsidentschaftswahlen an. Das Europäische Parlament wird im Juni neu gewählt, und Grossbritannien könnte voraussichtlich im Herbst ein neues Unterhaus bekommen. Gegen Jahresende kommt es in den USA dann zum Wahlknüller. Die Frage, ob in der Ukraine noch Präsidentschaftswahlen stattfinden werden, hat Selenskyj aufgrund des aktuellen Krieges noch offen gelassen.

Technologisch gesehen werden wir uns im neuen Jahr mit dem Thema KI weiter auseinandersetzen müssen. Denn eines steht fest: KI wird nicht nur fruchtbare Geschäftsmodelle hervorbringen. Die Gefahr, dass KI-gestützte Systeme von KI-generierten Daten lernen und kaputt trainiert werden, besteht allemal. Darüber hinaus werden Themen wie Cyber Threat Intelligence oder die militärische Notwendigkeit von Cyber wichtig bleiben. Wie sich Schweizer Firmen innerhalb der Cyberwelt aufstellen, und ob sie von vergangenen Fehlern lernen werden, wird sich dann im Verlaufe des Jahres zeigen.

Serena Bolt
Research Team

NEWS

WAS IST BEI UNS PASSIERT?



INTERVIEW AUF BLICK.CH ZU ACTIVE LISTENING

Marc Ruef konnte sich im Gespräch mit blick.ch zum Thema Active Listening austauschen und seine Sicht der Dinge teilen und sagt, dass ein gezieltes Abhören durch unsere Telefone durchaus möglich ist. Die Strafen, die von der DSGVO ausgehen, machen ein gezieltes Abhören jedoch sehr unattraktiv. Meistens stünde ein ausgeklügeltes digitales Marketing dahinter, da Nutzerinnen und Nutzer oftmals Daten mit Sozialen Plattformen teilen, ohne sich dessen bewusst zu sein.

INTERVIEW IM SRF ZUM DATENLECK BEI DER SCHWEIZER ARMEE

Erneut wurde eine Bundesbehörde Opfer eines Datenlecks, dieses Mal scheint die Schweizer Armee betroffen zu sein. Marc Ruef tauschte sich mit den Journalisten Conradin Zellweger und Nadine Woodtli über den Vorfall aus und erklärte, wieso ein Leck im militärischen und nachrichtdienstlichen Umfeld besonders kritisch ist. Es ist mittlerweile der dritte Hack auf Bundesdaten innerhalb der vergangenen 6 Monaten. Ruef sagt abschliessend, dass es bundessache sei, mehr Sicherheit von seinen Zulieferern einzufordern.

DIGITAL FOOD BUSINESS WEEK 2024

Marisa Tschopp konnte an der ZHAW am 8. Januar 2024 eine Vorlesung zum Thema KI aus psychologischer Sicht mit einem spezifischen Fokus auf Vertrauen im Rahmen der Digital Food Business Week 2024 in Wädenswil halten. Die Business Week erstreckte sich über die ganze Woche und thematisierte ganz unterschiedliche Bereiche, die von disruptiven Technologien bis zu Tokenization, Business Modelling und Digitale Transformation reichen.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

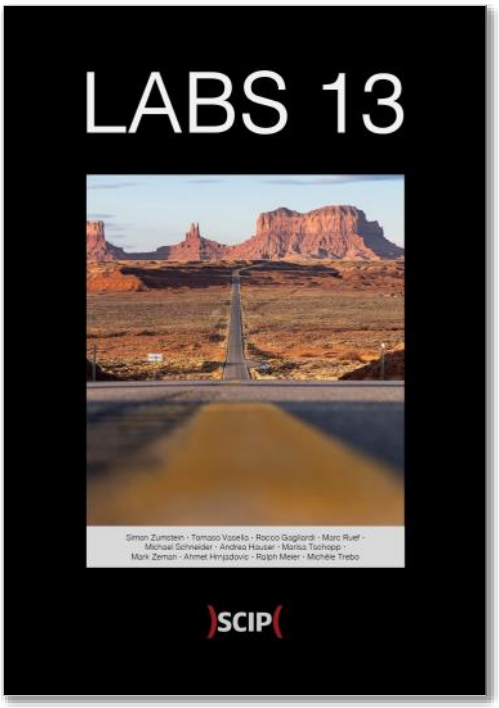
UNSER AKTUELLES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-30-4) als auch in englischer Sprache (ISBN 978-3-907109-31-1) verfügbar. Das Vorwort wurde von Dr. iur. David Vasella verfasst und setzt sich mit den rechtlichen Rahmenbedingungen der Informationssicherheit auseinander.

In unserem Katalog finden sich ebenfalls themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen auf unserer Webseite.



GEOPOLITIK IM CYBERRAUM: CHINA

Bilderquelle: https://unsplash.com/de/fotos/rotes-und-schwarzes-herz-illustration-Uo-roJMypEo

SERENA BOLT

CYBERGEFAHREN UNTER GEOPOLITISCHEN FAKTOREN: EIN BLICK AUF CHINA

In einer zunehmend vernetzten Welt, in der digitale Technologien einen zentralen Platz einnehmen, sind Cybergefahren zu einer bedeutenden Herausforderung geworden. Beinahe täglich sind Unternehmen und Privatpersonen von Cyberangriffen betroffen, bei denen die Angreifer vor allem eines wollen: Sich durch den Verkauf der erschleichen Daten finanziell bereichern. Die Gefahren, die durch Gruppierungen oder einzelnen Individuen ausgehen, gehen jedoch über gezielte Hackerangriffe hinaus: Auch staatliche Akteure, also Regierungen, haben ihre Interessen und setzen auf eine digitale Angriffsführung. In diesem ersten Artikel der Serie Cybergefahren unter geopolitischen Faktoren gehen wir der Frage nach, wie diverse Länder systematisch Cyberevents nutzen, um ihre geopolitischen Interessen durchzusetzen. Denn auch China nutzt für seine territorialen Fehden Spionageaktionen und Desinformationskampagnen, um seine Ziele zu erreichen. Doch was zeichnet das Reich der Mitte aus, und welche Motivation verfolgt Xi Jinping in dieser Sache?

ÜBER CHINA

China ist ein faszinierendes Land. Man denke an die imposante Chinesische Mauer, die Traditionen und Sprache, die Kultur, die Menschen. In den letzten Jahrzehnten hat sich China nicht nur zu einer globalen Wirtschaftsmacht entwickelt, sondern spielt mittlerweile auch eine tragende Rolle als grosser Technologieplayer. Alibaba, Tencent, Baidu und TikTok sind längst über die Landesgrenzen bekannt, und haben sich auch hierzulande zu beliebten Plattformen entwickelt. Doch China befindet sich immer wieder im Kreuzfeuer mit anderen Regierungen. Sei es um das technologische Wettrüsten mit den USA oder Schlagzeilen macht als Überwachungsstaat und der Verfolgung von Dissidenten. Mit über 1,4 Milliarden Menschen ist China das bevölkerungsreichste und flächenmässig drittgrösste Land der Erde. Die Wirtschaft wächst rasant, und Städte wie Peking und Shanghai sind moderne Metropolen, die dem Land zu rasantem technologischem Wachstum verhelfen.

- Einwohner: 1.4 Milliarden
- Hauptstadt: Peking

- Fläche: 9.6 Millionen km²
- Zeitzone: CST (China Standard Time). Fun Fact: Die Zeitzone erstreckt sich über das gesamte Land
- Sprachen und Dialekte: Mandarin (68%), Kantonesisch (5%), Shanghaiesisch, Hokkien, Tibetisch, Uigurisch, Mongolisch
- Staatspräsident: Xi Jingping
- Staatsform: Sozialistische Volksrepublik
- Regierungspartei: Kommunistische Partei der Volksrepublik (80 Millionen Mitglieder)
- Oppositionspartei: Keine Oppositionsparteien
- Verwaltungsstruktur: Zentralregierung in Peking, 22 Provinzen, 5 autonome Regionen, Sonderverwaltungszonen Hong-Kong & Macau

CHINA UND SEINE TECHNOLOGIESTRATEGIE

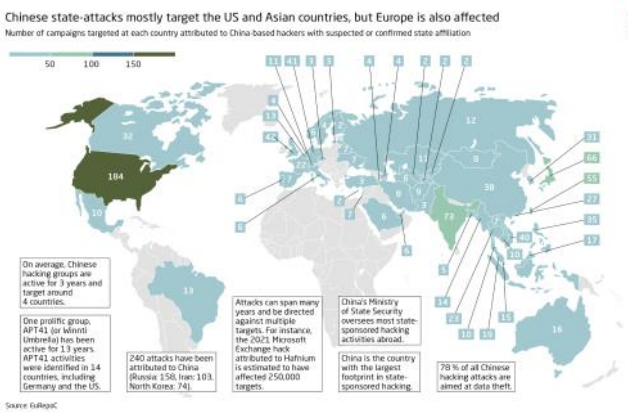
Wieso bietet aber gerade China einen fruchtbaren Boden für neue technologische Entwicklungen, die gut (oder sogar besser) mit dem internationalen Standard mithalten können? Nun, diese Frage hat mit verschiedenen Begebenheiten zu tun, hängt unter anderem aber mit zwei grundlegenden Faktoren zusammen: Erstens mit den massiven Aufwendungen in KI-Systeme, und zweitens der umfangreichen Datensammlung ihrer eigenen Bevölkerung. Dabei ist das Ziel klar: Bis 2030 will das Land zur weltweit führenden KI-Macht werden. Geplant sind Investitionen von rund 15 Milliarden US Dollar, was einem Anstieg von 50% innerhalb zweier Jahren entspricht. Die chinesische KI Strategie, die im New Generation AI Development Plan festgelegt wurde, zielt eine Marktentwicklung von etwa 150 Milliarden USD an, und will KI demnach auch armeefähig machen.

Das chinesische Militär PLA (Chinese People's Liberation Army) will zudem Marschflugkörper, unbemannte Luftfahrzeuge, Control & Command Systeme sowie die Überführung von ziviler KI-

Unternehmen in die Armee einbringen, die die intelligente Kriegsführung Chinas beschleunigen sollen. Mit Command und Control Systemen hat sich Peking zum Ziel gesetzt, die Planung und Durchführung von Luft-, Raumfahrt-, Cyberspace-, See- und Landoperationen zu zentralisieren. Darüber hinaus soll in Wuhan eine Cyber-Hochburg errichtet werden, bei welchem China Experten im Bereich Cybersicherheit für die Armee ausbilden lässt. Wuhan soll generell ein nährbarer Boden werden für innovative Unternehmungsgründungen und vermehrt als Schauplatz nationaler Hacking-Wettbewerbe fungieren.

Da die Regierung mittlerweile über Jahrzehnte Daten über ihre Bevölkerung sammelt, analysiert, über eine Milliarde Überwachungskameras im Land installiert hat, bietet es eine optimale Grundlage für das Trainieren zahlreicher Algorithmen und Modelle. Diese begünstigen Chinas Aufschwung angesichts KI-Technologien massiv. Das ganze mündet dann im sogenannten China Social Score System, bei welcher die chinesische Bevölkerung durch die umfangreiche Datenerfassung ihrer Regierung erfasst und bewertet wird.

Doch die Augen der Volksrepublik sind nicht nur auf die eigene Bevölkerung gerichtet: Auch andere Länder gelangen ins Visier Chinas. So sollen nationalstaatliche Akteure international relevante Unternehmen mit gezielten Cyberattacken und Spionage bespitzeln, um die Strategien ihrer Mitbestreiter in Erfahrung zu bringen. Im Microsoft Digital Defense Report 2023 zählt der US-amerikanische Konzern diverse Institutionen auf, die Opfer von chinesischen Hackern wurden. So gehört beispielsweise die US-amerikanische Verteidigungs- und Rüstungsindustrie, diverse Kommunikationsunternehmen im Bereich Cloud und IT-Sicherheit sowie staatliche Unternehmen zu ihren präferierten Zielobjekten dazu.



Natürlich könnte man argumentieren, dass die USA ein gewisses Eigeninteresse hegt, solche Beschuldigungen gezielt an China zu richten, um vor ihren eigenen Motiven abzusehen. Doch eine vertiefte Auseinandersetzung, ob jetzt Washington Peking angreift oder umgekehrt, würde der Rahmen dieses Artikels sprengen.

Ungeachtet des Tech-Wettrüsten mit den USA liegen jedoch auch andere Länder im Visier der chinesischen Regierung, wie ein Abbild aus der Analyse China Security and Risk Tracker von Merics hervorgeht.

CHINA UND SEINE STAATLICHEN AKTEURE

In der Welt der Cybersicherheit spricht man von unterschiedlich motivierten Akteuren, die allesamt verschiedene Ziele verfolgen. Nationalstaatliche Bedrohungsakteure haben vor allem eine Vision: Die Pläne und Informationen ihrer Kontrahenten besser zu verstehen, und um sich mit dem Informationsvorsprung einen strategischen Vorteil zu verschaffen. Cyberspionage ist daher auch in China ein weit verbreitetes Tool zur Überwachung und Bespitzelung.

Das können einerseits Zivilisten sein, die für die jeweiligen Regierungen, Nachrichtendienste oder das Militär arbeiten. Andererseits auch Hackergruppen, die von Staaten und Regierungen rekrutiert worden sind (oder von diesen finanziert werden). Sie sind unter anderem auch als ATPs bekannt, sogenannte Advanced Persistent Threats, die man als Art Projektgruppe innerhalb des Nachrichtendienstes oder eben des Militärs ansehen kann. Sie sammeln systematisch Informationen, und sind meistens über einen längeren Zeitraum mit der Überwachung ihrer Ziele beschäftigt. Obwohl sie mit komplexen Instrumenten und spezialisiertem Cyber-Know-how agieren, sind ihre Aktionen alles andere als profitabel, denn sie interessieren sich in erster Linie für die Informationsbeschaffung und die Störung von Verfügbarkeit und Handlungsfähigkeit.

Eine chinesische Hackergruppierung muss also nicht unbedingt eine direkte Verbindung zur Regierung aufweisen, aber die Indizien deuten darauf hin, dass sie dennoch mit der PLA oder dem Ministerium für Staatssicherheit oder dem Ministerium für öffentliche Sicherheit verbandelt sind. In China sind mehre-

re ATPs unterwegs. 2023 agierten vor allem diese zwei Gruppierungen:

- **Raspberry Typhoon:** zielt auf militärische Einrichtungen und Unternehmen ab, die kritische Infrastrukturen betreiben. Ihre Masche sind Spear-Phishing Massnahmen, um ihre Malware zu streuen.

- **Flax Typhoon:** Die Gruppierung hat es auf kritische Infrastrukturen in Taiwan abgesehen, vor allem in Richtung medizinische Einrichtungen, Medienhäuser, Verteidigung und Auftragnehmer, welche eng mit den USA arbeiten. Man geht davon aus, das dass Sammeln spezifischer Informationen dabei ihr Hauptinteresse ist.

Raspberry Typhoon sammelt dank gezielten Spear-Phishing Kampagnen Informationen, um dann ihre Malware zu streuen. Seit Beginn 2023 zielt die Gruppierung nun auf Ministerien, welche im Bereich Handel oder im Finanzwesen angesiedelt sind. Auch Nachrichtendienste gehören zu den potenziellen Interessengruppen von Raspberry Typhoon. Flax Typhoon im Gegensatz arbeitet mit VPN-basierten Lösungen, um sich beliebig Zugang zu den Netzwerken zu schaffen, um so seine Opfer auszuspionieren.

CHINA UND SEINE GEOPOLITISCHEN KONFLIKTE

Bevor wir einzelne geografische Konfliktherde aus China näher erläutern, ist folgendes wichtig zu verstehen: Man kann nie genau wissen, ob diese Angriffe tatsächlich von gewissen staatlichen Gruppierungen ausgehen, oder wer genau hinter diversen Cyberangriffe steckt. Denn das legen falscher Fährten, sogenannter false flags, ist auch in der digitalen Welt eine verbreitete Taktik, um vor dem eigentlichen Handeln abzulenken. Nehmen wir nun einige Beispiele genauer unter die Lupe die aufzeigen, dass zwischen Chinas geopolitischen Konflikten und ihren Cyberangriffen durchaus einen validen Zusammenhang besteht.

TAIWAN UND DAS SÜDCHINESISCHE MEER

Man geht davon aus, dass China gezielte Cyberangriffe auf andere Regierungen unternimmt, um hauptsächlich Desinformationskampagnen zu streuen und sich mittels Cyberspionage Informationen zu

beschaffen. Dies ist in Taiwan nicht anders. Vor allem mit dem Inselstaat ist der Territorialkonflikt äusserst umstritten, der nun seit mehr als 70 Jahren andauert. Es ist wohl einer der grössten Reibungsflächen zwischen China und den USA, und obwohl Taiwan eigentlich ein unabhängiges Land ist, wird es bislang nur von 12 Staaten offiziell anerkannt. Abgesehen von geografischen Gegebenheiten hat China auch ein weiteres wirtschaftliches Interesse, dass Taiwan offiziell in die Volksrepublik integriert wird. Taiwan ist nach wie vor führend in der Produktion von Halbleitern weltweit, welche man für die Produktion von Computerchips verwendet. Die jahrelangen Territorialkonflikte im südchinesischen Meer bleiben nach wie vor ungeklärt, da viele Länder in der Region dieselben Seegebiete und Inseln für sich beanspruchen. Diese ungewisse Ausgangslage motiviert China zusätzlich, neben Taiwan auch in Staaten wie Malaysia oder Indonesien zu intervenieren und dort seinen Einfluss zu sichern.

Wenn man sich untenstehende Grafik genauer anschaut fällt auf, dass sich chinesische Cyberevents zwischen Juli 2022 und Juni 2023 auf verschiedene Regionen im südchinesischen Meer erstrecken, und sich nicht nur ausschliesslich auf Taiwan fokussieren.

DIE VEREINIGTEN STAATEN UND GUAM

Nicht nur das südchinesische Meer wird dabei ins Visier genommen: Auch die USA verzeichnete im vergangenen Jahr deutlich mehr Cyberattacken, die der chinesischen Regierung zugesprochen werden könnte. Allen voran soll China seine Spionageaktivitäten auf die USA ausweiten, um eine sogenannte neue Seidenstrasse, der New Belt Road, mit der dazugehörigen Regionalpolitik vorwärts zu bringen. Spannend zu erwähnen ist die geografische Lage der westlichen Pazifikinsel Guam, welches zwar 12'000 Kilometer von Washington D.C. entfernt liegt, jedoch offiziell als Aussengebiet der USA dazugehört.

doch offiziell als Aussengebiet der USA dazugehört. Guam beheimatet derweil der US Luftwaffenstützpunkt Andersen Air Force Base, und dient darüber hinaus auch der US Navy als Marinestützpunkt. Sollte es tatsächlich zu einem Konflikt zwischen China und den USA kommen, so könnte Guam ein wichtiger geografischer Hub werden, zumal die Insel auch von gegnerischen Akteuren schnell erreichbar wäre.

RUSSLAND

China kämpft auch mit dem nördlichen Nachbarn Russland um umstrittene Gebiete. Die Volksrepublik hat gegen Sommerende 2023 seine Landesgrenzen neu aufgezeichnet, und dabei die nordöstliche Insel Bolschoi Ussurijski neu sich selbst zugewiesen, obwohl die Region zu Russland gehört. Es handelt sich um etwa 100 km² neues Territorium; der Besitzanspruch der Insel wurde von russischen Seiten jedoch nie bestätigt. Dabei kommt die Frage auf, ob der Territorialkonflikt beim Amur-Fluss zu einer erneuten Krise zwischen China und Russland führen könnte. Da der Kreml seit dem Krieg gegen die Ukraine jedoch grosszügig von Peking mit Autos und Elektronik beliefert wird, geht man nicht davon aus, dass sich Putin gegen Xi querstellen wird. Wie lange sich das Spiel zwischen den beiden Machthabern hält, wird sich zeigen.

INDIEN

Im Zuge der intern angestrebten neuen Landkarte hat die Regierung Chinas ebenfalls die Grenze zu Indien um 3500 km² für sich beansprucht. So wurde der Bundesstaat Arunachal Pradesh von der Regierung Chinas in Süd-Tibet umbenannt. Die Bergregion Aksai Chin, welche sich westlich von Tibet befindet, wird ebenso von China reklamiert.

AFRIKA

Der afrikanische Kontinent landet immer wie mehr in den Fokus der Desinformationskampagne Chinas. Google geht in seinem Cybersecurity Forecast für 2024 davon aus, dass der Grund für Spionageaktivitäten auf afrikanische Institutionen vor allem ressourcenbedingt sind. Seltene Mineralien werden für technische High-End Geräte wie Smartphones, TVs, Laptops sowie Hybrid- und Elektroautos verwendet und sind daher für die dazugehörige Produktion

unverzichtbar. So könnte China seine wirtschaftliche und strategische Position in Afrika durchaus stärken. Durch die finanzielle Unterstützung autoritärer Regimes hätte China eine weitere Taktik, ihre Desinformationskampagne weiter zu streuen. Hinzu kommt, dass im äthiopischen Addis Abeba mit Hilfe der chinesischen Regierung das Hauptquartier der Afrikanischen Union errichtet und technologisch ausgestattet wurde. Die Afrikanische Union hat sich als Ziel gesetzt, durch Zusammenarbeit nachhaltiger Frieden, Sicherheit und Wohlstand für den gesamten Kontinent zu sichern. Die AU wurde zwischen 2013 und 2018 mehrmals Opfer von gezielten Cyberattacken, die ihren Ursprung in China haben könnten, und ein ähnliches Bild zeichnet sich auch in Burundi und Nigeria ab.

AUSBLICK UND FAZIT

Nationalstaatliche Bedrohungsakteure wie im Falle Chinas sind durchaus eine Ernst zu nehmende Angelegenheit. Das Jahr 2024 mit seinen entscheidenden Ereignissen wie die Olympischen Spiele in Paris, die Wahlen des Europaparlaments, die Präsidentschaftswahlen in den USA oder Wahlen in Ländern wie Taiwan, Südkorea, Russland, Indonesien und Indien werden mit Sicherheit ideale digitale Angriffsmöglichkeiten bieten. Vor allem in Taiwan spitzt sich die Lage aktuell zu, denn am 13. Januar 2024 finden auf der Insel Präsidentschafts- und Parlamentswahlen statt. Dass Xi Jinping deshalb Druck auf die dortige Gesellschaft ausüben will, liegt aufgrund seiner Bestrebungen zur Wiedervereinigung auf der Hand. Chinas geopolitische Interessen im südchinesischen Meer wären hinsichtlich Wahlprogramm in Taiwan jedoch Argument genug, Cybervorfälle aus der Volksrepublik genauer zu beobachten.

Darüber hinaus hat sich Xi Jinping mit Made in China 2025 zum Ziel gesetzt, verstärkt auf die inländische Innovationskraft zu setzen, um die eigene Techszene voranzukurbeln und das Land zum Top Tech High-End Produzent zu machen. Kombiniert mit den KI-Bestrebungen des Landes werden wir im 2024 ebenfalls chinesische Aktivitäten im Rahmen von Cyberspionage, Dissidentenverfolgung und Streuung von Falschinformationen erleben. So voraussagt es zumindest Google in seinem Cybersecurity Forecast für 2024.

Nationalstaatliche Bedrohungen hören aber nicht in Peking auf: Auch Russland, Israel oder Nordkorea befinden sich seit Jahrzehnte im Territorialstreit mit anderen Staaten. Die aktuelle Krise im Nahen Osten und in der Ukraine zeigen beispielslos auf, wie physische Konflikte längst in die digitale Kriegs- und Angriffsführung übergegangen sind. Und obwohl China vielleicht andere Ziele verfolgt als Russland oder andere Regierungen: Mit ihren zahlreichen geografischen Reibungsflächen, dem illegalen Annektieren von grenznahen Gebieten und dem Wahn nach geografischer und politischer Macht wird sich Chinas Regierung auf lange Sicht wohl keine Freunde machen.


Serena Bolt

Sie brauchen Unterstützung? Wir sind Ihre Partner für professionelle Cybersecurity Services.

RALPH MEIER

BURP BAMBDAS & BCHECKS: NEUERUNGEN IN DEN LETZTEN MONATEN

In unseren Web Application Penetration Tests verwenden wir hauptsächlich Burp Suite Professional als Machine-in-the-Middle Proxy, um uns bei unseren Tests zu unterstützen und diese so effektiver durchführen zu können. In den letzten Monaten kamen zwei grössere Features zu Burp Suite hinzu: Bambdas und BChecks. Im Rahmen dieses Artikels schauen wir uns diese zwei Neuerungen genauer an, deren Einsatzzweck und einige Einstiegsbeispiele.

BAMDBAS

Die Bezeichnung Bambdas setzt sich aus einer Kombination von Burp und Lambda zusammen. Bambdas ermöglichen Anwender von Burp Suite ihr Tool beziehungsweise deren Funktionalität auf einfache Weise direkt auf der grafischen Benutzeroberfläche mittels Java Codestücken zu erweitern. PortSwigger möchte damit eine Möglichkeit bieten, Burp in sämtlichen Punkten von Benutzern erweitern zu können. Bisher war dies nur durch die Entwicklung von Burp Extensions möglich, welche mehr an Entwicklungs-Know-how wie zum Beispiel den Umgang mit Build Tools wie Maven oder Gradle voraussetzten.

AKTUELLER STAND

Bambdas wurden mit der Veröffentlichung von Burp Suite Release 2023.10.3 eingeführt. Als erstes wurden Bambdas im Proxy Tab eingeführt und ermöglichen so das Filtern von HTTP Traffic. Somit brachte PortSwigger zuerst eine Erweiterung des HTTP History Filters. Ein Bambda wird an dieser Stelle auf ein HTTP History Item (requestResponse Item) angewendet und kann somit sämtliche Eigenschaften der durchgeführten Requests und dazugehörige Responses abfragen, filtern und hervorheben. Im bisherigen Filter der HTTP History konnten reguläre Ausdrücke eingesetzt werden, jedoch sind Bambdas deutlich mächtiger und umfangreicher. Nun ist es auch möglich, ein regulär konfigurierter Filter in ein Bambda zu konvertieren und dies mit Java Code zu erweitern. Im Bambda Mode lassen sich bereits fertige Bambdas hineinkopieren, aus Dateien importieren oder direkt im Editor entwickeln sowie zu einem späteren Zeitpunkt speichern. Zum Zeitpunkt dieses Labs wurden Bambdas im WebSockets Histroy Filter und in der Filterfunktion im Logger Tab in einer Early Adopter Version von Burp Suite bereits veröffent-

licht. Der stable Release wird wohl in den kommenden Wochen folgen.

ANWENDUNGSBEREICHE & BEISPIELE

Mit Bambdas im Proxy HTTP Traffic Filter lassen sich spezifische Endpunkte, Requests mit Inputfelder, spezielle Header oder andere Anomalien aus allen History Items filtern und hervorheben. Damit lassen sich Sonderfälle einfach eingrenzen und anschliessend einzeln untersuchen. Da Bambdas aus Java Code sind, besteht die Möglichkeit von Exceptions bei der Ausführung. Im Falle von Exceptions wird dies in Burp angezeigt und beim Öffnen des Filters werden detailliertere Informationen inklusive Stack-Trace dargestellt.

BEISPIEL EINER NULLPOINTEREXCEPTION IN EINEM BAMBDA

Mit Bambdas können zum Beispiel Requests welche /resources/ oder /image/ im Request Path beziehungsweise der URL enthalten ausgeblendet werden. Gleichzeitig können interessante History Items wie jene die /api im Request Path haben grün und solche die die /graphql beinhalten gelb eingefärbt werden. Im folgenden Beispiel werden noch zusätzlich History Items, welche im Request Path .js enthalten sind, in der Farbe Magenta eingefärbt.

```
String requestPath = requestResponse.request
().pathWithoutQuery();

if(requestPath.isBlank()){
   return false;
}
if(requestPath.contains("/resources/") ||
requestPath.contains("/image/")){
   return false;
}

if(requestPath.contains("api")){
   requestResponse.annotations
().setHighlightColor(HighlightColor.GREEN);
}

if(requestPath.contains("graphql")){
   requestResponse.annotations
().setHighlightColor(HighlightColor.YELLOW);
```

```
}
if(requestPath.contains(".js")){
   requestResponse.annotations
().setHighlightColor(HighlightColor.MAGENTA);
}
return true;
```

Bambdas können ebenfalls zum Filtern von eingesetzten Server-Response-Headern verwendet werden, wie zum Beispiel Server oder X-Powered-By. Anschliessend kann manuell geprüft werden, ob es sich bei dem Ergebnis um eine Offenlegung von Informationen handelt.

```
// in case of no response
if (!requestResponse.hasResponse()) {
   return false;
   }
var response = requestResponse.response();
// Header Server or X-Powered-By is present
if (response.hasHeader("Server") ||
response.hasHeader("X-Powered-By")){
   String headerServer = response.headerValue
("Server");
   if(headerServer==null ||
headerServer.isBlank()){
      return false;
   }
} else {
   return false;
}
return true;
```

Im Vorstellungsartikel von PortSwigger zu Bambdas sind noch weitere Beispiele zu finden. PortSwigger führt zudem ein eigenes Github Repository für Bambdas, welches von Anwender gerne erweitert werden darf.

ZUKÜNFTIGE ENTWICKLUNG

In Zukunft möchte PortSwigger die Erweiterbarkeit von Burp mittels Bambdas an zusätzlichen Orten wie in die zentrale Suchfunktion integrieren. Ein Vorfiltern bei Intruder-Attacken ermöglichen, sowie Bambdas in den Capture Filter beim Logger und bei HTTP Listeners einbauen. Ziel soll es sein, mehrere einfache Bambdas kombinieren zu können, um so komplexe Aufgaben in einem Tool durchzuführen.

BCHECKS

Der in Burp Suite integrierte Scanner bringt bereits von Haus aus eine grosse Anzahl an Scanchecks für ein breites Spektrum von bekannten Schwachstellen wie SQL-Injections, Cross-Site-Scripting, XML-Injections und viele weitere. Mit BChecks soll der integrierte Scanner auf eine einfache Art direkt in Burp Suite selbst mit eigenen Checks erweitert werden können. Produktspezifische Schwachstellen sind in den mitgelieferten Scanchecks oft nicht enthalten, können daher mittels BChecks selbst hinzugefügt werden.

AKTUELLER STAND

Mit dem Release 2023.6.2 von Burp Suite wurden BChecks hinzugefügt. Diese befinden sich innerhalb des Extensions Tabs und können dort importiert, erstellt und verändert werden. Im letzten stable Release vor der Publikation dieses Artikels (2023.11.1.3) kam noch Syntax highlighting im BChecks Editor hinzu. Auch für BChecks pflegt PortSwigger ein Github Repository. Mit dem Early Adopter Release 2023.12.1 kam eine Formatier Funktion für BChecks hinzu, diese ist mittels Rechtsklick im Editor durchführbar.

ANWENDUNGSBEREICHE & BEISPIELE

Mittels BChecks können Prüfpunkte für produktspezifische Schwachstellen erstellt werden, welche noch nicht in Burp Suite enthalten sind, einige Beispiel können im Artikel von PortSwigger gefunden werden. BChecks können auch eingesetzt werden, um nicht optimal gesetzte Server-Response-Header festzustellen, im folgenden Beispiel geht es um die Konfiguration des HTTP Strict-Transport-Security Header. Der Code kann direkt unter folgendem Link eingesehen werden: https://www.scip.ch/?labs.20240111.

Bei der Entwicklung von BChecks kann die BCheck Definition Reference von PortSwigger enorm helfen, da sie einen guten Gesamtüberblick über die Möglichkeiten und Informationen über die notwendigen Teile eines BChecks enthält. Weitere Beispiele können im BChecks Repository von PortSwigger gefunden werden.

BCHECKS TESTING TOOL

Im Release 2023.10.2.2 von Burp Suite wurde die Möglichkeit BChecks zu testen ausgeliefert. Das Testen von erstellten oder importieren BChecks findet im BChecks Editor statt. Dafür werden History Items aus der HTTP Proxy History via Send to BCheck editor, was neu im Rechtsklick Kontextmenü in der HTTP Proxy History zu finden ist, als Test Case beim BChecks Editor hinzugefügt. Anschliessend kann im BCheck Editor der ausgewählte BCheck auf die selektierten Test Cases mittels Run Test angewendet werden. Das Ergebnis kann danach in den Tabs Audit items, Event Log, Logger und die aus dem BCheck erstellen Schwachstellen im Issue activity Tab angeschaut werden. Diese Testing Methode wurde eingeführt, um herauszufinden wieso false Positives aus einem BCheck entstehen und ihn dahingehend zu verbessern und einfach erneut anwenden zu können.

ZUKÜNFTIGE ENTWICKLUNG

Über die zukünftige Entwicklung und Erweiterung von BChecks ist aktuell nichts bekannt.

FAZIT

Mit BChecks lassen sich schnell eigene Checks für produktspezifische Schwachstellen entwickeln und einsetzten. Die Einführung von Bambdas in Burp hilft Benutzern das Filtern von History Items exakter zu steuern und ihre persönlichen Vorlieben in der Hervorhebung einfach und automatisch durch den erstellten Bambdas umzusetzen. Die Einführung von Bambdas an weiteren Orten ist sehr vielversprechend und fördert kleine Automatisierungen und benutzerspezifische Anpassungen, ohne die Entwicklung von dedizierten Extensions vorzunehmen. Neben Bambdas und BChecks unterstützt Burp Suite auch Makros, damit hat sich Andrea im Artikel Burp Makros – Wie sie korrekt verwendet werden auseinandergesetzt.

Ralph Meier

Bildquelle: https://unsplash.com/de/fotos/blau-weisse-und-rote-abstrakte-malerei-NTYYL9Eb9y8

SCIP MONTHLY SECURITY SUMMARY

IMPRESSUM

ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Marc Ruef

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion des Herausgebers, den Redaktoren und Autoren nicht übernommen werden. Die geltenden gesetzlichen und postalischen Bestimmungen bei Erwerb, Errichtung und Inbetriebnahme von elektronischen Geräten sowie Sende- und Empfangseinrichtungen sind zu beachten.

ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

Weder Unternehmen noch Redaktion erwähnen Namen von Personen und Firmen sowie Marken von fremden Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch