Online-Version anzeigen

BIGS

BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

BIGS-Newsletter 4/2018

Sehr geehrte/r Damen und Herren ,

zwar beschäftigen wir uns am BIGS überwiegend "nur" mit ökonomischen Fragen von Cybersicherheit, dennoch wird insbesondere mein Kollege Alexander Szanto immer wieder gefragt, was man selbst tun kann, um den eigenen Schutz im Cyberraum zu erhöhen. Mit diesem Newsletter beginnt er eine kleine Reihe mit Tipps und Tricks, die wir in den kommenden Monaten fortführen wollen. Den ersten Teil finden Sie hier.

Wer sich dafür interessiert, wie man Extremismus, "Hate Speech" und "Fake News" auf Internetplattformen bekämpft und welche Regulierung der entsprechenden Technologieunternehmen hierzu erforderlich sind, der ist herzlich am Donnerstagabend in das Haus der Bundespressekonferenz eingeladen. Gemeinsam mit dem Counter Extremism Project (CEP) veranstaltet das BIGS eine **englischsprachige Diskussionsveranstaltung am 29.11. um 18 Uhr** mit einem einleitenden **Vortrag von Prof. Hany Farid von UC Berkeley**. Mehr Informationen zu unserer Veranstaltung und die Möglichkeit sich anzumelden finden Sie hier.

Ganz ohne Hate Speech wünsche ich Ihnen eine hoffentlich ruhige Adventszeit.

Mit besten Grüßen aus Potsdam

Ihr
Dr. Tim Stuchtey

Newsletter Reihe zum Thema Cyber Sicherheit

Wie kann ich mich und meine Daten vor dem Zugriff durch Cyber Kriminelle schnell, unkompliziert und wirksam schützen?

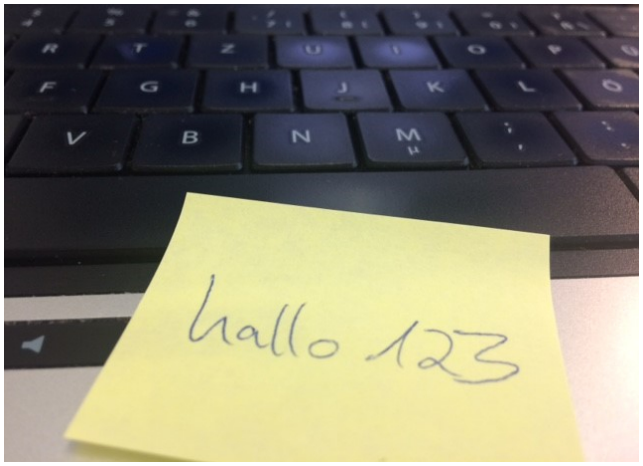
Digitale Erpressung, Datendiebstahl durch Social Engineering, Identitätsdiebstahl und Passwortdiebstahl durch Phishing, sowie massenhafte Fernsteuerung von Computern (sogenannte Botnets) sind Deliktbereiche, die wie kaum ein anderer Bereich eine kontinuierlich steigende Kriminalitätsentwicklung verzeichnen. Laut einer repräsentativen Befragung von 1.017 Internetnutzer im Auftrag des Digitalverbandes Bitkom von Oktober 2017wurde jeder zweite Internetnutzer in den letzten 12 Monaten Opfer von Internetkriminalität. Dabei erstatte nur jeder sechste Betroffene Anzeige bei der Polizei. Die Polizeiliche Kriminalstatistik selbst zeigt zwar steigende Fallzahlen im Bereich Internetkriminalität auf, die Dunkelziffer dürfte jedoch weitaus höher sein als die 251.617 Fälle, die 2017 mit dem Tatmittel Internet in Verbindung stehen.

Die Schäden gehen dabei in die Milliarden und es gibt nur eine Tendenz: nach oben. Genaue Zahlen lassen sich nicht nennen, da viele Cyber Angriffe erst sehr spät oder gar nicht entdeckt werden. Im Sommer letzten Jahres äußerte sich der Präsident des Bundesamtes für Verfassungsschutz (BfV), Hans-Georg Maaßen, besorgt und schätzte den Schaden durch Cyber Angriffe auf jährlich 50 Milliarden Euro.

Der entscheidende Faktor für die Vielzahl von erfolgreichen Cyber Angriffen ist nach wie vor der Mensch. Technische Schutzmaßnahmen können noch so gut sein; wenn Menschen an entscheidender Stelle aus Sorglosigkeit oder Nachlässigkeit versagen, sind sie nutzlos.

Da Sicherheit mehr als nur Technik ist, wollen wir als BIGS in den kommenden Ausgaben einige Sicherheitsmaßnahmen vorstellen, die Sie als Nutzer schnell, unkompliziert und wirksam umsetzen können, um Ihre Daten vor fremdem Zugriff zu schützen. Mit bereits einfachen Mitteln und Maßnahmen können Sie das Sicherheitsniveau Ihrer Daten und Online-Accounts erheblich verbessern und zudem sicherstellen, nicht jedem Cyberkriminellen auf den Leim zu gehen.

#1: Einführung in das Passwortmanagement



Die Zahl unserer Online-Konten ist in den letzten Jahren rasant gestiegen. Musik hören, die nächste Reise vorbereiten, das passende Outfit für die Hochzeit besorgen, Lebensmittel einkaufen, die Überweisung für das Gruppengeschenk, fast alles ist heutzutage auch, oder nur noch online möglich. Mit jedem neuen Service, den wir online nutzen, benötigen wir ein Konto und somit auch ein Passwort. Und genau dies hat sich in letzter Zeit als Problem herausgestellt. Täglich hören wir in den Nachrichten von Cyberkriminellen, denen es gelungen ist, auf unterschiedliche Art und Weise an Kundendaten zu gelangen. Dabei spielen häufig eher die kleinen Details eine Rolle, also die ganz großen systematischen Schwachstellen. Ein effektives **Passwortmanagement** kann dabei helfen, diese Hürden für Kriminelle heraufzusetzen und Nutzerkonten sicherer zu machen.

Der Mensch ist ein Gewohnheitstier und dies zeigt sich auch bei der Auswahl der Passwörter. Eine erst kürzlich veröffentlichte Studie hat eine umfassende empirische Analyse der Wiederverwendung von Passwörtern durchgeführt und einige beunruhigende Ergebnisse geliefert. Der Sicherheitsexperte Wang und seine Kollegen analysierten in der Studie „The Next Domino Fall: Empirical Analysis of User Passwords across Online Services“ die Wiederverwendungs- und Änderungsmuster von Passwörtern, indem sie einen Datensatz von 28,8 Millionen Nutzern und deren 61,5 Millionen verwendet werden und dass Modifikationen aufgrund ihrer geringen Varianz leicht vorhersehbar sind. Experten warnen immer wieder vor der Verwendung einfacher Passwörter, die leicht zu erraten sind oder durch spezielle Algorithmen relativ schnell geknackt werden können. Ein Passwort, viele Konten. Dieses Problem betrifft nicht nur unsere privat genutzten Konten, denn aus Gründen der Bequemlichkeit gibt es häufig keine allzu großen Unterschiede zu denen, die im beruflichen Gebrauch sind.

In den letzten Jahren machten immer wieder Meldungen über riesige **Datenlecks** die Runde, darunter so bekannte Namen wie MySpace und LinkedIn. Die Mehrfachverwendung von Passwörtern schafft somit ein hohes Risiko für Internetnutzer mit weitreichenden Folgen. Wenn Sie überprüfen möchten, ob Ihr Passwort noch sicher ist oder bereits im Netz kursiert, können Sie dies zumindest teilweise auf der Internetseite Pwned Passwords abfragen.
In dieser Datenbank sind mehr als eine halbe Milliarde Passwörter hinterlegt, die bei Datenschutzverletzungen bereits exponiert wurden. Findet sich Ihr Passwort dort wieder, sollten Sie es unverzüglich ändern und eine Mehrfachnutzung vermeiden. Das Hasso-Plattner-Institut (HPI) bietet einen ähnlichen, kostenlosen Service an. Der HPI Identiy Leak Checker überprüft Ihre E-Mail-Adresse und gleicht sie mit Daten ab, die im Internet veröffentlicht wurden. So können Sie überprüfen, ob

Passwörtern in 107 Diensten über einen Zeitraum von acht Jahren untersuchten. Die Datensätze waren vorher entwendet und öffentlich zugänglich gemacht worden. Durch den Abgleich mit den E-Mail-Adressen konnten die Forscher die verschiedenen Datensätze und somit auch die zugewiesenen Passwörter miteinander vergleichen. Zu den wichtigsten Erkenntnissen der Untersuchung gehört, dass 38% der Nutzer ihr Passwort mindestens einmal in zwei verschiedenen Diensten wiederverwendet und 21% sie nur leicht modifiziert haben.
Des Weiteren zeigt die Studie auch, dass Passwörter selbst nach einem Datendiebstahl noch jahrelang Ihre Identitätsdaten im Internet offengelegt bzw. missbraucht wurden.
Sollten Sie jedoch zu den Nutzern gehöre, die einfache Passwortkombinationen wie „123456“ verwenden (diese Zahlenfolge hat das Hasso-Plattner-Institut in einer Studie von 2016 als das meistbenutze Passwort in den untersuchten Daten-Leaks identifiziert) , oder Passwörter wie „hallo“, „hallo123“, „qwertz“ usw. benutzen, ist eine Überprüfung redundant.
Mit diesen Kennwörtern steht jedem potentiellen Datendieb der Zugriff auf Ihre Konten offen. Sie sollten aus diesem Grund folgende Faustregeln berücksichtigen:

Verwenden Sie **Passwörter mit mehreren Zeichen**, wenn möglich 10 und mehr.

Verwenden Sie **keine persönlichen Daten,** z.B. Namen und Geburtsdaten von Freunden und Verwandten oder von Ortschaften und Unternehmen, mit denen Sie in Verbindung stehen.

Kombinieren Sie Buchstagen mit Zahlen, Groß- mit Kleinschreibung, Sonder- mit Satzzeichen.

Versuchen Sie, wenn möglich, alle paar Monate Ihr **Kennwort zu ändern** und verzichten Sie auf nur leichte Modifikationen.

Verwenden Sie, wenn vorhanden, die **Zwei-Faktoren-Authentifizierung** (wird mittlerweile auf vielen Online-Plattformen angeboten), um zu verhindern, dass Kriminelle nach dem Diebstahl ihrer Passwörter Zugriff auf die Konten erhalten.

Wenn Sie diese Vorgehensweise beherzigen, ist ein Missbrauch ihrer Konten zwar nicht völlig ausgeschlossen, Sie reduzieren das Risiko jedoch beträchtlich.
In der nächsten Ausgabe stellen wir Ihnen einige Passwort Manager vor, die den Umgang mit vielen verschiedenen Online-Konten und Passwörtern erleichtern und Ihnen eine Menge Arbeit ersparen.

Wir wünschen Ihnen eine sichere Woche
Ihr BIGS Team

Brandenburgisches Institut für
Gesellschaft und Sicherheit
Dianastr. 46
14482 Potsdam
info@bigs-potsdam.org