Inhaltsverzeichnis:

1. Aktuelle Gefahren/Bedrohungen/ Hinweise

1.1 Millionenfacher Identitätsdiebstahl von Zugangsdaten zu E-Mail-Konten

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen millionenfachen Identitätsdiebstahl von E-Mail-Kontodaten samt Passwörtern aufgedeckt. Mindestens 16 Millionen E-Mail-Konten sollen „gestohlen“ worden sein – an die Daten gelangten die Kriminellen auch über mit Malware infizierte Rechner.

Das BSI und die Polizei raten daher:

- Testen Sie Ihre E-Mail-Adressen auf der eigens beim BSI eingerichteten Prüfseite https://www.sicherheitstest.bsi.de/
- Sollte Ihr E-Mail-Postfach betroffen sein, bereinigen Sie Ihren Rechner entsprechend den Hinweisen des BSI.
- Ändern Sie die Zugangsdaten des kompromittierten Postfachs und aller anderen Profile, wenn Sie gleiche Zugangsdaten verwenden.
- Beachten Sie die Hinweise für die sichere Vergabe von Passwörtern beim ProPK (http://www.polizei-beratung.de/sicherheitskompass/sicheres-passwort) oder BSI (https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html).

Quellen:
BSI (https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Mailtest_21012014.html)

Heise online (http://www.heise.de/security/meldung/BSI-Mehrere-Millionen-Internet-Konten-durch-Botnetze-geknackt-2090167.html)

1.2 Thema: Hacktivismus

Cybercrime ist ein Phänomenbereich, der sehr breit gefächert ist und im Rahmen der relevanten Strafnormen des StGB eine Reihe von verschieden motivierten Delikten umfasst. Ein recht neues und medial sehr präsentes Phänomen ist der so genannte Hacktivismus.

Hacktivismus verbindet Hacking mit dem Geist des Protestes und den damit einhergehenden neuen Arten des sozialen Umgangs seit dem Ende des 20. Jahrhunderts. Die Motivation der als Hacktivisten bezeichneten Täter begründet sich häufig in politischen und ideologischen Zielen, wobei die Täter Mittel der modernen Kommunikation und das Hacking nutzen, um ihre Begehrlichkeiten und Ziele zu vermitteln und durchzusetzen.

Hacktivisten unterscheiden sich dabei von Cyberterroristen[1], Internetaktivisten[2], Cyberspionen und -saboteuren[3] und durch Zueignungsabsicht motivierten Cyberkriminellen. Hacktivisten verfolgen

[1] Die Nutzung des Internets durch Terroristen zur Ausführung von Angriffen und als Kommunikationsplattform (Propaganda). Gewalt ist das Ziel, wohingegen Hacktivismus gewaltlos ist.
[2] Internetaktivisten vertreten einen netzpolitischen Aktivismus zur Gestaltung, Nutzung und Regulierung des Internets in einem gesellschaftlich wünschenswerten Sinne z. B. als Kampf gegen Zensur, für Zugang zum Netz und im Sinne der Urheberrechtsproblematik, wobei das Internet z.B. als Diskussions-, Kommunikations- und Informationsmittel zur Mobilisierung von Anhängern dient.
[3] Täter, die im Rahmen der sog. Cyber-Kriegsführung, bei der mindestens eine offizielle Regierung beteiligt ist, Infrastrukturen ausspionieren oder sabotieren.

keine gewinnorientierten Ziele, bewegen sich durch die eigenen Handlungen aber dennoch in einem strafbewährten Handlungsraum, denn sie nutzen Datennetze nicht auf legalem Wege, um ihre Ideologien und Zielsetzungen zu verbreiten. Die Handlungen der Hacktivisten können aber auch durch Spaß am Hacking oder die Gewinnung von Anerkennung und Respekt in der Szene motiviert sein. Tätertypologien sind sehr heterogen.

Die prominenteste Gruppierung, die dem Hacktivismus zugeordnet wird, ist ANONYMOUS. Ihre Akteure finden prinzipiell anlassbezogen zusammen und treten meist im typischen Erscheinungsbild – der Guy-Fawkes-Maske – mit ihren Aktionen in den Medien auf und scheinen dem Prototyp des Hacktivisten zu entsprechen. Die objektive Situation dieses kriminalstatistisch nur sehr schwer mess- und darstellbaren Phänomens sieht indes so aus, dass es eine nicht bestimmbare Zahl von scheinbaren Gruppierungen gibt, die ideologische Ziele auf illegalem Wege vornehmlich im Internet publizieren.

Die Modi Operandi gestalten sich vielschichtig und jeder im Internet aktive Nutzer kann Opfer der Hacktivisten bzw. zu einer Plattform für deren Proteste und Propaganda werden. Das offensichtlich am häufigsten gewählte Mittel der Täter ist das so genannte Web-Defacement. Die Täter nutzen dabei Sicherheitslücken auf Webseiten bzw. in Web-Content-Management-Systemen aus: Sie dringen in die Systeme ein, verändern die dort befindlichen Dateien für ihre Inhalte, so dass die ursprünglichen Webseiten nicht mehr oder verändert angezeigt werden. Es wird angenommen, dass solche Webseiten nicht bewusst ausgewählt werden, sondern dass gezielt nach lückenhaften Plattformen für die Angriffe gesucht wird.

Ein weiteres wichtiges Instrument der Täter ist die Distributed-Denial-of-Service-Attacke (DDoS). Mittels speziell programmierter Tools und meist unter Nutzung von sog. Bot-Netzen[4] starten die Hacktivisten groß angelegte Angriffe auf die Webseiten ihrer Opfer, die hier gezielt ausgewählt und angegriffen werden. Ziel ist es, Zeichen zu setzen und Maßnahmen beim Opfer zu erzwingen, die den Zielen der Täter entsprechen. Bei diesen Attacken beteiligen sich oft Dritte, die bewusst oder unbewusst als Teil des Botnetzes mit ihren Datenanfragen an die betroffene Webseite zum Angriff beitragen.

Des Weiteren spähen Hacktivisten auch Online-Konten politischer Gegner aus, um diesen mit den gewonnenen Erkenntnissen zu schaden oder dessen Reputation zu schwächen. Die finanziellen Schäden hacktivistischer Straftaten lassen sich allerdings kaum beziffern, da eine dezidierte Erfassung der Straftaten kaum möglich ist. Einer mangelnden Anzeigenbereitschaft der Opfer wie auch der Schwierigkeit, Taten und Tatversuche überhaupt zu entdecken, ist es zuzuschreiben, dass die quantitative Darstellung des Phänomens nur sehr bedingt möglich ist.

Jeder im Internet aktive Nutzer kann Opfer der Hacktivisten werden. Sei es als Betreiber einer Webseite, sei es als Nutzer von E-Mail oder sozialer Netzwerke. Hat das eigene System Lücken, entspricht das

[4] Ein vom Straftäter geschaffenes Netz von Computern, die durch eine Infizierung von Malware als sog. Zombie-Rechner dem Ziel des Täters dienlich sind und von dessen Command&Control-Server gesteuert werden.

Passwort nicht den gängigen Sicherheitsstandards oder geht man allzu leichtfertig mit Downloads und dem Besuch dubioser Internetseiten um, so findet man sich schnell als Geschädigter einer Szene wieder, die es versteht mit einfachen Mitteln und Know-how politische und ideologische Ziele im Internet zu publizieren und klarzumachen, dass man in der Lage ist, Schäden zu verursachen und politische Gegner zu schwächen.

Die Polizei rät daher:

- Halten Sie Betriebssystem und Anwendungssoftware, wie Browser und Content-Management-Systeme stets auf neuestem Stand.
- Behalten Sie Ihre Webseiten und Profile in sozialen Netzwerken im Auge, um auf Veränderungen und Manipulationen schnellstmöglich reagieren zu können.
- Zeigen Sie Straftaten gegen IT-Infrastrukturen und persönliche Daten bei der Polizei an.
- Beachten Sie die Vorgaben zu Passwortsicherheit. Vergeben Sie nie dasselbe Passwort für mehrere Anwendungen. Das gilt insbesondere für Dienste im Internet – und ändern Sie das Passwort in regelmäßigen Abständen.
- Nutzen Sie die Medien des Programms Polizeiliche Kriminalprävention der Länder und des Bundes zur Förderung von Mediensicherheit und empfehlen Sie diese weiter.

Quelle:
Bundeskriminalamt, KI 16, Projekt Hacktivisten

2. Ins Netz gegangen – Ansätze polizeilicher Kriminalprävention zum Schutz vor Internetkriminalität

Schadsoftware, Fake-Shops oder Kostenfallen – das Internet hat neben vielen Vorzügen auch Schattenseiten. Auch durch das „mobile“ Netz dank Smartphone und Tablet steigt das Risiko, im Internet Opfer einer Straftat zu werden. Beinahe täglich tauchen neue Betrugsvarianten auf, die mittels Internet verübt werden. Auf diese Entwicklung reagiert auch die Polizeiliche Kriminalprävention – und entwickelt stetig neue zielgruppenspezifische Instrumente zur Vorbeugung. Diese gehen über die reine Vermittlung von Medienkompetenz hinaus und rücken den Sicherheitsaspekt beim Umgang mit digitalen Medien in den Vordergrund.

Ob es ein Flyer, eine Handreichung für pädagogische Fachkräfte oder ein Beitrag im polizeilichen Newsletter ist – das Programm Polizeiliche Kriminalprävention der Länder und des Bundes geht viele Wege, um Privatpersonen, Fachleute, Unternehmer oder Journalisten über die Gefahren im Internet, im Sozialen Netzwerk oder bei der Smartphone-Nutzung zu informieren. Im Mittelpunkt steht dabei immer der sichere Umgang mit den Neuen Medien – auch Mediensicherheit genannt. Gemeint sind damit die sicherheits- und polizeilich relevanten Aspekte der Mediennutzung. Eingeschlossen sind Handlungen mit rechtlichen Bezügen als auch solche, die eher in einer Grauzone zwischen legal und illegal stattfinden, wie die Veröffentlichung von Bildern anderer in sozialen Netzwerken. In Abgrenzung dazu bezeichnet „Medienkompetenz“ die Fähigkeit einer Person, Medien sinnvoll zu nutzen, wobei der Schwerpunkt nicht speziell auf Sicherheitsaspekten liegt.

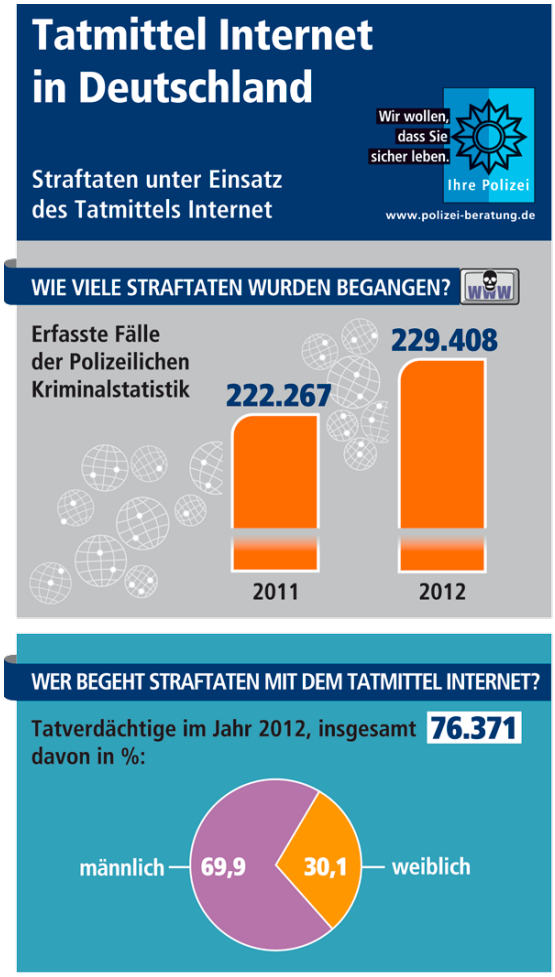
Unter dem Leitbegriff **Mediensicherheit** veröffentlicht das ProPK Informationen, die den Nutzer über Internetkriminalität aufklären und ihm Wege aufzeigen, wie er sich selbst schützen kann.

Hilfestellung und Praxisbeispiel in einem ist die Online-Anwendung **„Sicherheitskompass“**. Dieser wurde von ProPK und dem BSI bereits vor rund zehn Jahren entwickelt und vermittelt Regeln zu den zehn häufigsten Sicherheitsrisiken im Internet. Moderner gestaltet und mit praktischen Video-Tipps angereichert zeigt der „Sicherheitskompass“ wie jeder Nutzer sich durch technische Mittel und richtiges Verhalten vor Internetproblemen und -kriminalität schützen kann.

Die **Sammelmappe „Klicks-Momente“** informiert Internetnutzer über Gefahren und Risiken beim Umgang mit Computer, Smartphone und Co. Die Mappe enthält Faltblätter zu Themen wie Betrug im Internet, Sicherheitsrisiken bei der Nutzung von Smartphones oder Sozialen Netzwerken. Tipps, die auch weniger geübte Nutzer befolgen können, zeigen Schutzmöglichkeiten auf. Um die strafrechtliche Relevanz einiger Inhalte zu verdeutlichen, enthalten die Faltblätter auch Auszüge aus Gesetzestexten.

Ausgangslage und Polizeiliche Erkenntnisse

Dass Mediensicherheit seit vielen Jahren ein Schwerpunktthema des bundesweiten Vorbeugungsprogramms der Polizei ist, hängt naturgemäß stark mit der Entwicklung der registrierten Fallzahlen zusammen. Im Jahr 2012 wurden in der Polizeilichen Kriminalstatistik für Deutschland 229.408 Straftaten mit dem **Tatmittel Internet** festgestellt, 2011 waren es 222.267 Fälle. Darunter fallen Deliktsformen wie Waren- oder Computerbetrug, die Verbreitung pornografischer Schriften oder Straftaten gegen Urheberrechtsbestimmungen. Hinzu kommt, dass in die-



sem Deliktsbereich von einem großen Dunkelfeld ausgegangen werden muss, weil viele Betroffene den Weg zur Polizei scheuen – oft auch weil ihnen die Aussicht auf Erfolg einer Strafanzeige eher gering zu sein scheint.

Fest steht, dass alle Zielgruppen (Jugendliche, Erwachsene, Senioren, Unternehmer) gleichermaßen von Internetkriminalität und abweichendem Verhalten (Grauzone) betroffen sind. Das zeigen repräsentative Befragungen und Studien wie die KIM- und JIM-Studie oder Untersuchungen des Branchenverbands BITKOM[5].

Die **Risiken**, denen User ausgesetzt sind, lassen sich in drei Bereiche klassifizieren:

- inhaltlich (Pornografie / Kinderpornografie, Gewalt, Betrug),
- kommunikationsbezogen (Cybermobbing, Cyber-Grooming[6], Identitätsdiebstahl) und
- technisch (Hardware-Sicherheit, Schadsoftware).

Nutzer können beispielsweise Opfer und/oder unbewusst Mittäter von Vermögensdelikten, Opfer von Beleidigungen sowie abweichendem Verhalten an der Grenze zur Strafbarkeit werden. Hinzu kommt, dass Täter in der vermeintlichen und tatsächlichen Anonymität des Netzes agieren und Neugier, Leichtgläubigkeit und Unvorsichtigkeit der Opfer ausnutzen. Kleine und mittelständische Unternehmen können von Vermögensdelikten und Wirtschaftsspionage betroffen sein. Auch die

[5] Die KIM-Studie (Kinder und Medien) sowie die JIM-Studie (Jugend, Information, (Multi-)Media) werden vom Medienpädagogischen Forschungsverbund Südwest (MPFS) herausgegeben. Der Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (BITKOM) führt regelmäßig Befragungen zum Nutzungsverhalten durch.

[6] Das gezielte Ansprechen von Personen im Internet mit dem Ziel der Anbahnung sexueller Kontakte.

schnelle Entwicklung der digitalen Medien fordert von Nutzern fundierte Kenntnisse der Schutzmöglichkeiten. Häufig jedoch fehlt es an der nötigen Sensibilität für sicherheitsrelevante Aspekte bei der Nutzung moderner Kommunikationsmittel. Dieses Bewusstsein bei Internetnutzern zu schaffen, ist ein entscheidender Teil der polizeilichen Präventionsarbeit und findet sich in den programmatischen Zielen wieder.

Ziele der Präventionsmaßnahmen
Um den unterschiedlichen Gefahren mit spezifischen Präventionsempfehlungen begegnen zu können, hat sich ProPK folgende Ziele gesetzt, nach denen die Präventionsangebote ausgerichtet werden.

- Fachkompetente und zielgruppengerechte Präventionsangebote auf den Internetseiten des ProPK, vor allem auf www.polizei-beratung.de, sollen über inhaltliche, kommunikationsbezogene und technische Risiken aufklären und Schutzempfehlungen vermitteln. Zielgruppen sind nicht nur Privatpersonen und Unternehmer, sondern auch die Polizei.
- Durch die Präventionsangebote sollen die Zielgruppen sich besser vor Gefahren und Straftaten bei der Nutzung der Neuen Medien schützen können.
- Kompetente Kooperationspartner tragen durch ihr Fachwissen zur Qualität der veröffentlichten Informationen und Medien bei.

Kleiner Überblick über die Prävention heute und morgen

Um die gesetzten Ziele zu erreichen, sind unterschiedliche Ansätze unverzichtbar. Einer davon ist eine kontinuierliche Presse- und Öffentlichkeitsarbeit. Da praktisch täglich neue Gefahren auftauchen, neue Tatbegehungsweisen bekannt werden, muss die Information darüber und die Vermittlung von Schutz- und Sicherheitsempfehlungen „just in time“ erfolgen.

Durch eine intensive Öffentlichkeitsarbeit kann die Polizei neue Varianten und Begehungsweisen sowie die dazugehörigen Schutzempfehlungen schnell aufzeigen. Daher hat sich auch die **Presse- und Öffentlichkeitsarbeit des ProPK** immer mehr zu diesem Themenfeld hin entwickelt. Dies spiegelt sich nicht nur auf der **Internetseite** www.polizei-beratung.de wider. Begleitend zu den auf der Webseite eingestellten Hinweisen erscheinen Pressemeldungen oder Newsletter für Bürger und Journalisten.

Aber auch interne Wege der Informationsvermittlung sind von Inhalten rund um Internetgefahren und Mediensicherheit geprägt: Polizeiintern werden die Kolleginnen und Kollegen mit vorliegendem IT-Newsletter regelmäßig über neue Risiken und Gefahren sowie über Schutzmöglichkeiten informiert. Dadurch werden die Ansprechpartner der Bürger auf den neuesten Stand gebracht und können so Betroffenen vor Ort hilfreich zur Seite stehen.

Bei der Förderung der Mediensicherheit bei Kindern und Jugendlichen können Eltern, Lehrkräfte sowie Präventionsfachleute der Polizei eine unterstützende und beratende Rolle spielen. Dafür hat das Programm Polizeiliche Kriminalprävention bereits zahlreiche Medien entwickelt und bereitet derzeit gemeinsam mit dem BSI auch ein **neues Medienpaket** (Film-DVD und Begleitheft) vor. Dieses soll u. a. im Schulunterricht oder im Rahmen polizeilicher Vorträge vor der Zielgruppe eingesetzt werden. Das Medienpaket erscheint voraussichtlich März 2014.

Im Programm der Polizeilichen Kriminalprävention bereits etablierte Medien werden weitergeführt. Dazu gehört beispielsweise die Handreichung „Im Netz der neuen Medien“. Sie informiert über die Gefahren, denen Kinder und Jugendliche im Umgang mit dem Internet, Handy und Computerspielen ausgesetzt sind, und wird an Lehrer, Erzieher und pädagogische Fachkräfte ausgegeben. Die Handreichung ist nun in einer 4. aktualisierten Auflage erschienen.

2006 wurde die Kampagne „Kinder sicher im Netz“ gemeinsam mit der Deutschen Telekom AG und der Freiwilligen Selbstkontrolle Multimedia (FSM) gestartet. Ziel dieser Kampagne ist, Kinder, Eltern, Lehrer und andere Erziehungsverantwortliche für die Gefahren im Internet zu sensibilisieren. Zentraler Baustein dieser Kampagne sind Spots mit Bastian Schweinsteiger und Rudi Cerne, die konkrete Tipps zur Förderung sicherheitsbewussten Verhaltens geben.

Die gemeinsame Initiative „Online Kaufen - mit Verstand“ von eBay, dem Bundesverband des Deutschen Versandhandels (bvh) und dem ProPK, hat das Ziel, vor Betrug bei Onlinekäufen zu schützen und den Wissensstand über sicheren Online-Handel zu erhöhen.

Die vielen Anstrengungen und Bemühungen haben letztendlich ein Ziel: Sie sollen jeden Internetnutzer dazu befähigen, sich sicher in der virtuellen Welt bewegen zu können. Denn das Internet hat neben den Schattenseiten eben auch viele Vorzüge.

Quelle: Programm Polizeiliche Kriminalprävention der Länder und des Bundes

Medien des ProPK zu Mediensicherheit

Klicks-Momente Internetnutzer
Download unter: http://www.gsbl.extrapol.de/propkmedienportal/

Suchauswahl:
Thema: Computer-/Internetkriminalität
Medienart: Sonderformat

Sicherheitskompass
unter www.polizei-beratung.de/sicherheitskompass

Weitere Medien erhalten Sie im ProPK-Medienportal unter: http://www.gsbl.extrapol.de/propkmedienportal/