SOPHOS

Die Anatomie Tätertypen auf der digitalen Seite der Macht

Wer sind diese Typen, die man „Hacker“ nennt?

Sophos beschreibt die gängigsten Hackertypen

Part 1: Fünf Hackertypen, die vor allem Endverbraucher bedrohen

Wiesbaden, 14. März 2016 Hacker sind mal wieder in aller Munde. Sie greifen Staaten, Unternehmen, Einrichtungen, wie zuletzt Krankenhäuser und auch Endverbraucher an. Wer sind diese mysteriösen Typen? Was treibt sie an, was können sie? Sophos beschreibt die 5 wichtigsten Hackertypen, von denen vor allem Endverbraucher bedroht werden und empfiehlt Maßnahmen zum Schutz.

1. Die verbreitetste Plage: Der digitale Kleinkriminelle

Bei den digitalen Kleinkriminellen handelt es sich wahrscheinlich um die größte Hackergruppe. Diese Hacker-Spezies besteht aus Personen mit ganz unterschiedlichen Fähigkeiten und Techniken, die manchmal auch in Gruppen organisiert sind. Allen ist gemeinsam, dass sie es ausschließlich auf das Geld ihrer Opfer abgesehen haben. Arglose Benutzer in ihre Netze zu locken und deren Computer oder Daten für kriminelle Zwecke zu missbrauchen, gelingt ihnen dabei meist mit den folgenden sechs Methoden: Spam, Phishing, Black-Hat SEO, Drive-by-Downloads, Malware und **Ransomware**. Besonders letztere ist

derzeit sehr stark anzutreffen. Sie wird genutzt, um nach unerlaubtem Eindringen und etwa Versperren oder Verschlüsselung der Daten vom Besitzer für deren Wiederfreigabe ein „Lösegeld “ zu fordern. Trafen diese Angriffe in der Vergangenheit hauptsächlich Privatpersonen, so ist aktuell ein steigender Trend zu fast schon professionalisierter Erpressung von Unternehmen erkennbar.

Möglicher Schutz: Auf dem Weg zum Geld müssen die Täter stets eine ganze Reihe von Arbeitsschritten hinter sich bringen. Wird nur ein einziges Glied in dieser Abfolge durchbrochen, kann ihnen bereits das Handwerk gelegt werden. Wer konsequent möglichst sofort alle verfügbaren Updates installiert, unnötige Anwendungen deinstalliert und bei normalen Benutzern auf Administratorrechte verzichtet, der vereitelt bereits über 90 Prozent dieser Angriffe.

2. Mal schauen, was geht: Der Spaß-Hacker

Der Spaß-Hacker, auch **Script-Kiddie** genannt**,** möchte einfach nur mal ausprobieren, ob ein „Script“ funktioniert. Er bricht mit Hilfe von vorgefertigten Scripten über ein Netzwerk in fremde Computer ein und richtet durch absichtlich verbreitete Schadprogramme – Viren, Würmern oder Trojaner – teilweise erheblichen Schaden an. Dieser Hacker ist überwiegend nur neugierig oder hat einen ausgeprägten „sportlichen“ Ehrgeiz. Finanzielles Interesse treibt ihn nicht an.

Eine **Untergruppe** der Freizeit-Hacker sind die so genannten **Cheater** im Bereich des Online Gamings. **Cheater** legen es darauf an, den Rest der Community um den Spielspaß zu bringen. Dafür nutzen sie illegale Hilfsprogramme, um sich in Spielen Vorteile (zum Beispiel durch besondere Fähigkeiten) zu verschaffen. Schutzmechanismen haben die Online

Gamer dagegen kaum; hier sind die Spiele- und Konsolenhersteller gefragt, bessere Schutzmechanismen in ihre Produkte einzubauen.

Möglicher Schutz: Regelmäßig Patches für den Rechner und Server durchführen, keine veraltete Software einsetzen und insbesondere Browser, Browser-Plugins und das Betriebssystem mit Updates aktuell halten, keine dubiosen Webseiten besuchen und auf keinen Fall auf Anhänge und Links unbekannter E-Mail-Absender klicken.

3. Im Auftrag Ihrer Majestät: Der Späher und Sammler

Der Späher und Sammler nutzt jede Möglichkeit, ununterbrochen und bei jedem digitalen Kommunikationsvorgang an Daten – auch Verbindungsdaten – heranzukommen. Hier sind echte Profis am Werk. Dahinter stecken nicht nur staatliche Ermittler und Geheimdienste, sondern auch große Konzerne, die sich für die digitalen Gepflogenheiten ihrer Kunden interessieren. Zwar entsteht bei der Massendatensammlung kein direkter Schaden, doch können diese Aktivitäten eine erhebliche Verletzung der Privatsphäre darstellen und bedeuten unter Umständen einen massiven Eingriff in die Bürgergrundrechte. Die Motivlage bei staatlichen Angriffen ist dabei eher unklar. Oft wird die Verhinderung von Straftaten als Begründung herangezogen. Die Motive großer Konzerne hingegen sind offensichtlich: Informationen über Kunden sind bares Geld wert. Bei gründlicher Analyse der von den Nutzern von Online-Diensten oftmals freiwillig offengelegten Daten lässt sich zum Beispiel Werbung für den Kunden haargenau anpassen.

Möglicher Schutz: Der beste Schutz vor Sammlern ist ein kritischer und bewusster Umgang mit den eigenen Daten. Personenbezogene Daten – insbesondere Adresse, Geburtsdatum und Bankdaten – sollte man nur dann angeben, wenn man der Webseite vertrauen kann. Für Online-Einkäufe gilt: möglichst Sammeldienste

verwenden, um die Streuung der eigenen Daten im Netz zu verhindern. Auch hat man hat mittlerweile die Möglichkeit, die Privatsphäre-Einstellungen bei Google, Facebook & Co. zu ändern, um so festzulegen, was gespeichert werden darf und was nicht. Auch Programme, die anonymes Surfen ermöglichen, helfen gegen Abschöpfung privater Daten. Das derzeit effektivste Mittel gegen Sammler und Späher ist die Verschlüsselung. Eine perfekte Anonymität gibt es derzeit jedoch nicht. Ein erster Schritt hierzu könnte ein moderneres EU-Datenschutzrecht sein.

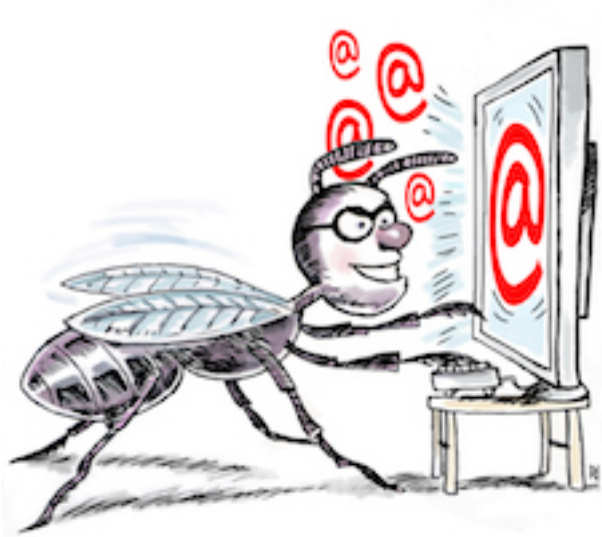
4. Der Smartphone-Hacker

Die Zahl der Smartphone-Nutzer in Deutschland hat mittlerweile die 45-Millionen-Marke überschritten. Smartphones sind dabei ständig in Betrieb und gespickt mit äußerst sensiblen Daten. Aber nach wie vor schützen sich die Anwender nur schlecht, so dass die Geräte immer häufiger von Hackern angegriffen werden: Smartphone-Hacker habe es auf Daten und Geld abgesehen. Dafür verwenden sie zumeist Schadprogramme, Viren und Trojaner, um physikalischen Zugriff auf die Geräte zu bekommen. Gängig sind aber auch Phishing- und Snoopware-Methoden. Da in der Regel die meisten Menschen den Weg des geringsten Wiederstands gehen, Smartphone-Hacker eingeschlossen, sind einfachere „Angriffe“, ohne gravierend auf Technik zu setzen, sehr in Mode gekommen: Social Engineering – Hacking auf zwischenmenschlicher Ebene.

Möglicher Schutz: Dass ein Smartphone einen Virus bekommen kann, ist den wenigsten Anwendern bewusst, und so werden zumeist auch nur wenige Schutzmaßnahmen (Viren-Scanner, aktuelle und vertrauenswürdige Software) eingesetzt. Hierdurch ist es für Hacker ein Leichtes, Sicherheitslücken auszunutzen. Deshalb sollte auf Smartphones auf jeden Fall eine Sicherheitssoftware als

Basisschutz installiert werden. Auch öffentliche WLANs können Fallen sein, über die Adressen geklaut oder das ganze Handy gesperrt werden kann. Auf den mobilen Geräten sollten nur bekannte und geprüfte Apps installiert werden – viele Apps versenden unbemerkt persönliche Daten. Smartphones sollten mit einem starken Passwort geschützt sein, das man sich gut merken kann und das kein Unbefugter kennt. Außerdem sollte man nicht vergessen, das automatische Einschalten des Lock-Bildschirms zu aktivieren, falls das Smartphone verloren geht.

5. „Ach wie gut, dass niemand weiß...“: Der Parasit



Der Parasit ist ein E-Mail Hacker, der am liebsten unter geklauter Identität agiert. „18 Millionen E-Mails gehackt“ – so oder ähnlich lauteten die Schlagzeilen, als im vergangenen Jahr Internet-Kriminelle 18 Millionen Mailadressen und Passwörter abgefangen haben. E-Mail-Hacking ist nach wie vor sehr beliebt, um auf fremde Kosten Online-Dienste zu nutzen, auf Shopping Tour zu gehen oder Spam zu versenden.

Der Parasit möchte eine andere Identität nutzen, um seinen kriminellen Machenschaften nachzugehen. Er hat ein rein finanzielles Interesse. Der E-Mail-Hacker hat sich auf das Knacken von E-Mails spezialisiert und verfügt über ein gewisses Maß an technischen Fähigkeiten. Mittlerweile gibt es sogar Anleitungen im Internet, wie man ein Passwort knacken kann. Im Laufe der Zeit hat er sein Vorgehen perfektioniert und er agiert im Hintergrund, so dass die Opfer den Schaden erst spät oder gar nicht bemerken.

Möglicher Schutz: Neben einem gesunden Misstrauen gegenüber unbekannten Absendern sollt man auf jeden Fall für „starke“ Passwörter (mindesten 8 Zeichen plus Sonderzeichen) sorgen und diese regelmäßig ändern. Auch sollte man auf keinen Fall auf Anhängen und Links unbekannter E-Mail-Absender klicken.

Die Illustrationen der hier genannten sowie weiterer Hackertypen finden Sie hochauflösend in unserer Presselounge:

http://www.tc-communications.de/presse_lounge/sophos.html

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de