NetSecure-IT
Next Generation Security

Neue Horizonte

Consulting für IT- und Cyber-Security
Informations- und Kommunikationssicherheitslösungen

Whitepaper Hackerdefinition

„Denke wie ein Hacker und Du weißt, wie Du Dich schützen musst"

NetSecure-IT
Next Generation Security

Consulting für IT- und Cyber Security

Informations- und Kommunikationssicherheitslösungen

W h i t e p a p e r

„Hackerdefinition“

Hacker (Motive) und Angriffstechniken

Die Definition Hacker nicht ganz richtig ist. Zu unterscheiden gilt Cracker und Hacker. Der Begriff wurde jedoch durch die Medien als Oberbegriff des Bösen eingebürgert. Der Begriff Hacker ist jedoch grundsätzlich Wertneutral anzusehen. Trotzdem bleiben wir des Verständnisses wegen selbst bei diesem Begriff. Der Begriff Hacker taucht erstmalig in den 50 gern Jahren auf und wurde mit einem Technik Enthusiasten verglichen. Verglichen auf heutige Zeit entspricht dies eher einem Computerspezialisten. Jeder, der offenen Quellcode verändert und es anschließend wieder der Allgemeinheit zur Verfügung stellt, ist demnach als Hacker zu bezeichnen. Die Gefahren im Netz und aus den eigenen Reihen werden immer noch stark unterschätzt. Unmissverständlich muss eines klar sein: Angriffe wird es immer geben und diese nehmen zu, nicht ab. Es wird ein Katz und Maus Spiel bleiben. Mit den richtigen Methoden können Gefahren jedoch minimiert werden.

Table of Content

Überarbeitet Januar 2015

Allianzen, denen Sie sich anschliessen können:

Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik und des Vereins BITKOM.

https://www.allianz-fuer-cybersicherheit.de/ | Deutschland

In der Melde- und Analysestelle Informationssicherung MELANI arbeiten Partner zusammen, welche im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen kritischen Infrastrukturen tätig sind.

Melde- und Analysestelle Informationssicherung MELANI | Schweiz

Was ist ein Hacker?

Es gibt 3 verschiedene Gruppen der Hacker zu unterscheiden.

Erstens der **White-Hat** (so viel wie „Weiße-Hütte") verwendet sein Wissen sowohl innerhalb der Gesetze als auch innerhalb der Hackerethik, beispielsweise bei Penetrationstests oder forensischen Test, denen ausdrücklich zugestimmt wurde. Oder eben für Dienstleistungen.

Zweitens der **Grey-Hat** (so viel wie „Graue-Hütte") verstößt womöglich gegen geltende Gesetze oder restriktive Auslegung der Hackerethik, allerdings zum Erreichen eines höheren Zieles. Beispielsweise durch veröffentlichen von Sicherheitslücken in Softwareprodukten. Oder eben zur Beweissicherung von Material, die vor Gericht verwendet werden könnten. Zu solchen Maßnahmen würde auch Forensik greifen müssen, wenn es sich um Beweismaterial handeln würde, was aber auch in Auftrag gegeben werden muss. Gilt jedoch nicht in allen Punkten.

Drittens der **Black-Hat** (so viel wie „Schwarze-Hütte") dieser handelt mit krimineller Energie in Beabsichtigung größtmöglichen Schaden anzurichten sowie Vandalismus zu betreiben und um evtl. Daten zu stehlen, bzw. gesagtes zur Wirtschaftskriminalität zu unternehmen. Er wird auch als Cracker bezeichnet.

Der **Black-Hat** hat demnach den Namen Cracker oder Datenräuber mehr als verdient, jedoch bleiben wir beim Begriff Hacker. Die Medien missachten diese Forderung nach Änderung. So tut dies natürlich auch die breite Masse.

Definition Hackerethik:

Die Hackerethik bezeichnet eine Sammlung ethischer Werte, die für die Hackerkultur ausschlaggebend sein sollen. Für diese Ethik gibt es mittlerweile verschiedene Definitionen, zentrale Werte in den verschiedenen Aufstellungen sind Freiheit, Kooperation, freiwillige und selbstgewählte Arbeit sowie Teilen. (Quelle: Wikipedia.org). Jetzt wissen Sie im groben, was ein Hacker ist. Deshalb können wir uns jetzt mit den Motiven dieser beschäftigen.

Welche Motive hat ein Hacker?

Motive gibt es viele. Dennoch möchten wir einige wichtige hier ansprechen. Zu unterscheiden gilt noch Belästigung und Verbrechen sowie die Definition eines schweren Hackerangriffs. Oft wird auch gesagt: „Kriminell oder genial?"

Es ist auch festzustellen, dass Hacker viel Geduld, Phantasie, Intelligenz und manchmal auch ihre eigene Welt mitzubringen haben. Hacker sind jedoch keineswegs Außenseiter wie manch einer denken würde. Wir behaupten, dass Hacker wichtig für unsere Gesellschaft sind.

Sie leben unter uns wie jeder andere normale Mensch auch. Hacker kommen auch mit den Merkwürdigsten und schlimmsten Pseudo Namen daher, um nur mal ein paar davon zu nennen als Beispiel: „Devil_Angel, Totschläger, Red_Hammer, BruteConnor, Cybertot, Osamabin_Death oder auch Terminator_Knife". Hinter jeder dieser Fassaden stecken Motive und auch Lebensgeschichten. Diese Pseudo Namen sind jedoch frei erfunden, tauchen aber in ähnlicher Form besonders in diversen Hacker Threads auf.

Ziel eines Hacks kann alles sein: Öffentliche Einrichtungen, Server, Drucker, Webseiten, Menschen im Allgemeinen und Politiker (z.B. Karl-Theodor zu Guttenberg als Kuchenminister), Chipkarten, Internetprotokolle, Satellitentelefone usw. und sofort. Die Liste würde Seiten füllen.

Es gibt dabei vier Gruppen zu unterscheiden:

Die, die nicht wissen, was sie tun, sind die schlimmsten. Man nennt sie auch "**Script Kiddies**". Sie benutzen fertige Software aus dem Internet und versuchen sich eines Hacks. Dabei verstehen sie die Angriffstechnik nicht und verursachen mitunter schwere Schäden. Diese Gruppe gehört auch zu den Internet-Vandalen, ist der jüngeren und unausgereiften Ausgabe der Hacker zuzuordnen, jedoch auch talentiert genug um solche Angriffe durchzuführen. Das heißt, diese Gruppe verfügt über genug Know-how auf technischer Basis.

Normalanwender und PC Kenner. Diese Gruppe ist weniger qualifiziert, von daher sind auch die Schäden weitaus geringer. Jedoch gibt es genügend Tools im Internet um auch dieser Gruppe Zugang zum Ausspionieren oder höherwertigem verhelfen kann.

IT-Professionals, weil Ihnen sehr umfangreiches Wissen zur Verfügung steht. Diese Gruppe weiß schon eher was sie tut, hat Basiswissen in hardwarenahen Programmiersprachen und kann abklären inwieweit Angriffe von statten gehen, hat auch Basiswissen über Verschleierungstaktiken und gängige Algorithmen. Wenn jedoch zu dieser Gruppe noch diverse Motive hinzukommen, zählt diese Gruppe mitunter zu einer gefährlichen Kategorie.

Die Vierte Gruppe sind die echten Spezialisten. Sie gehören zu den wenigen, die die Programme zum Angriff oder zum Aufspüren schreiben. Der **Black-Hat** dieser Gruppe weiß genau was er tut und kann mitunter schwerste Angriffe fahren.

Nun zu den Motiven:

Politische Motive

Politische Motive können sein, indem sich Gruppen outen, sie kämpften für die Freiheit der Bürgerinnen und Bürger des Landes. Die dabei erbeuteten Daten werden anschließend im Netz veröffentlicht. Man spricht hier auch vom Modernen Robin Hood. Außerdem heißen sie **Hacktivisten**.

So ist zum Beispiel der Zoll am 9.7.2011 von der Gruppe „No-Name Crew" angegriffen worden. Sie gaben politische Ziele für den Angriff bekannt. Der betroffene Server wurde nach dem Angriff abgeschaltet. Das Nationale Cyber-Abwehrzentrum wurde in Zusammenarbeit mit dem BSI eingeschaltet. Weitere politische Motive kommen auch von Aufträgen der Regierungen in aller Welt selber, um etwa Informationen eines anderen Landes zu erfahren. Zu nennen ist hier z.B. der Iran, der ausspioniert worden ist. Eine andere Form dieser Arbeit ist Wikileags.org, die jedoch zurzeit mit massiven wirtschaftlichen Mitteln zu kämpfen hat. Sie kämpfen auch für die Freiheit der Informationen, jedoch auf einer anderen Ebene.

Motiv Neugierde

Der Reiz dieser Sache ist oftmals bei Jugendlichen zu finden, die verschiedene Artikel gehört oder gelesen haben, um sich an der Sache zu versuchen. Die Befriedigung, ein bestimmtes System oder eine Organisation zu erobern oder einfach komplizierte Probleme zu lösen, steigert bei diesem Motiv enorm das Selbstwertgefühl, bzw. gibt das Gefühl etwas wert zu sein. Motiv kann auch sein, die kein liebevolles Zuhause haben oder die sich oft allein gelassen fühlen. Oftmals auch bei jugendlichen Straftätern zu finden. Ich sprach bereits von Sensibilisierung im Kindesalter. Denn diese Gruppe der Neugierigen weiß nicht so richtig was sie tut. Ein einfaches Beispiel:

Probieren, wie ich in des Nachbarn WLAN gelange. Software und Anleitungen dazu gibt es genug. Nicht nur im privaten Umfeld kommt Neugierde zur Geltung, sondern auch im Unternehmens Umfeld. Durch solche Neugierde können auch diverse (schwere) Schäden entstehen.

Motiv Anerkennung / Motivation

Ein weit verbreitetes Motiv ist das soziale Gefüge und dessen Rituale, was sich in das Gefüge des Neugierigen anreiht. Diese Gruppe möchte sich ein Ruf verschaffen unter seinesgleichen. Wir kennen das aus vergangenen Zeiten, das man eine Prüfung unter sich ablegen musste, um zu einer bestimmten Gruppe zu gehören. Unter den Gesichtspunkten heute ist es eben ein erfolgreicher Hack, um danach in die Mitte mit aufgenommen zu werden. Auch hier ist es die Anhebung des Selbstwertgefühls um entsprechend eine Wertstellung zu erreichen. Hier gilt auch die Sensibilisierung anzusetzen. Diese Gruppe verfügt jedoch schon über Erfahrung und gewinnt das Gefühl der Überlegenheit.

Motiv Machtgefühl

Das Gefühl alles kontrollieren zu können, bereitet einen besonderen Reiz unter den Hackern. Einzig und allein, das Wissen besitzen zu können, unsere Gesellschaft oder ein politisches System empfindlich treffen zu können spielt hier die größte Rolle dieses Motives.

Motiv Langeweile

Oftmals ist hier das Fehlen geistiger Stimulanz gegeben. Diese Gruppe fühlt sich unterfordert, z.B. in der Schule oder Studium. Sie suchen deshalb nach neuen Herausforderungen.

Das Robin Hood Motiv

Dieses Motiv ist eher bei jugendlichen Tätern zu finden. Diese wollen die Weltanschauung als Grund für das Hacken Angeben und sind verantwortlich in der Umverteilung von finanziellen Werten engagiert. Ein Beispiel aus den USA zeigte, dass dort von Hochrangigen Politikern, Gelder von deren Kreditkarten gebucht wurden und anschließend wohltätigen Zwecken zugutekommen ließen.

Motiv Sucht und Besessenheit

Auch hier gilt wieder die jugendliche Gruppe, die sich zu diesen Motiven bekennt. Oftmals hat diese Gruppe Probleme im Elterlichen Umfeld. Der PC wird damit zum Ersatz. Das Hacken wird zudem als Lebensgrundlage angesehen und mehr Zeit als im realen Leben damit verbracht. Dieses Motiv kann in schwerste Krankheitsbilder enden.

Motiv Finanzielle Bereicherung / Probleme

Dieses Motiv ist es wohl, was am häufigsten zu nennen ist. Habgier gehört auch zu diesem Motiv. Die Täter aus dieser Gruppe sind meist in kriminellen und auch realen Gruppen der Kriminalität zu finden. Meist stehen diese Täter unter finanziellem Druck und sind so angehalten ihre Finanzen auf diesen Wegen zu sanieren. Erpressung fällt ebenfalls in das Motiv dieser Gruppe. Ebenso die Vermietung von BOT-Netzen. (BOT-Netze / Betreiber illegaler Bot netze installieren die Bots ohne Wissen der Inhaber auf Computern und nutzen sie für ihre Zwecke.

Motiv Rache

Dieses Motiv ist nicht selten und kommt häufig unter ehemaligen Kollegen eines Unternehmens zum Tragen. Beispielsweise ist Herr Schulze von der Firma FinanzNot GmbH gekündigt worden. Herr Schulze rächt sich mittels eines Angriffs an seiner ehemaligen Firma. Das Befriedigt meist den Grund: ***So wie Du mir, so ich Dir***.

Motiv Ideologie

Hinter diesen Angriffen dieser Gruppen stecken staatliche, soziale und auch wirtschaftliche Organisationen deren Ruf geschädigt werden soll. Manche Hacker verstehen sich auch als Beschützer der Nation. Mit den Hacks wollen sie auch Ihre politische Meinung kundtun. Meist werden in dieser Gruppe Webseiten manipuliert und anschließend verändert wieder Veröffentlicht. (siehe Beispiel die Webseite zu Guttenberg als Kuchenminister). Es gibt jedoch noch weit mehr Motive, die Angriffe veranlassen können, jedoch sind dies die wichtigsten gewesen

Wer kann alles Hacken?

Wie wir bereits gesehen haben, geht es schon im Kindesalter und bei Jugendlichen los, die sich als Trittbrettfahrer versuchen eines Hacks zu begehen. Hacken kann demnach jeder, der bereit ist, sich das technische Wissen anzueignen, bzw. wer Interesse an dieser Technologie im Grunde besitzt.

Warum spricht man überhaupt von Hackergruppen?

Um Angriffe zu fahren, wird dies meist immer in Gruppen passieren, selten hört man von einzelnen Personen, wenn es sich um schwere Angriffe handelt. Das bedeutet, dass es so zu sehen ist, dass man es vorzieht im ***Kollektiv*** zu arbeiten. Ein Vergleich hierzu ist Beispielweise die BORG aus der **StarTrek** Reihe (***Next Generation***), die besagt, ***„Widerstand ist Zwecklos"***, **Ihr werdet alle assimiliert werden**". Ein einzelner Borg kann keinen Schaden anrichten, das Kollektiv sehr wohl.

Nur gemeinsam ist es stark. Das ist eigentlich das Prinzip, was hinter einer Hackergruppe zu verstehen ist. Wichtig ist es demnach zu wissen, dass Gewisse Organisationen in den USA dieses Prinzip verstanden haben und sich ebenfalls mit anderen Institutionen zusammengetan haben, um gezielt das Know-how auszutauschen, genau wie es die Hackergruppen auch tun. Man nennt dies auch **„Allianzen"** gründen. Jedoch wird es immer ein Katz und Mausspiel bleiben.

Wer oder was ist Anonymous?

Anonymous und LulzSec gehören zweifelsohne zur neuen Generation, wenn wir über Hacker sprechen.

Anonymous = Kollektiv / BORG = Kollektiv

Zur Anschauung ist einmal das Borg Motto hinter das Motto von Anonymous hinterlegt.

Anonymous stammt aus dem griechischen ab und bedeutet so viel wie der / die Namenlosen. Anonymous war anfangs als Spaßbewegung gedacht, jedoch trat diese Gruppe seit 2008 zunehmend politisch mit Protestaktionen für die Redefreiheit ein. Die Teilnehmer agierten anfangs nur im Internet, tuen es heute aber auch außerhalb. Zu erkennen sind sie durch ihre typische Maskierung. Aktionsmittel von Anonymous sind unter anderem Demonstrationen und (schwere) Hackerangriffe.

Das Motto von Anonymous lautet:

Wir sind Anonymous. *(Wir sind die Borg)*

Wir sind Legion / viele. *(Widerstand)*

Wir vergeben nicht. *(ist)*

Wir vergessen nicht. *(Zwecklos)*

Erwartet uns. *(Ihr werdet alle assimiliert werden)*

Verstehen Sie, was damit gemeint ist?

Die neuste Gruppe ist Lizard Squad. Sie verfolgen das Ziel des Black Hat, während Anonymous als moderner Robin Hood gilt.

Anfangs beschränkte sich Anonymous in seinen Forderungen hauptsächlich auf das Verbot der Church of Scientology und deren Praktiken und Institutionen. Der Glaube der Scientologen oder anderer Organisationen sollte dabei nicht angegriffen werden. In letzter Zeit richtet sich Anonymous immer mehr gegen Internetzensur sowie vom Staat ausgehende Zensur. Operationen sind unter anderem gewesen: Operation Payback, Operation Sony, Operation Zeta, Operation Tunesia, Operation Iran und weitere bedeutende Angriffswellen. Unter http://de.wikipedia.org/wiki/Anonymous_(Kollektiv) ist der Artikel in voller Länge nachzulesen. Die Internetseite in de von Anonymous http://du-bist-anonymous.de/

Was ist ein schwerer Hackerangriff?

Zunächst ein Auszug aus dem Tagesspiegel vom 15.07.2011

Kampf gegen Hacker

USA suchen Verbündete nach Attacke auf das Pentagon

Rund zwei Jahre hat das Pentagon an seiner neuen Verteidigungsstrategie für das Internet gearbeitet. Ein jüngst verübter, schwerer Hackerangriff zeigt, wie bitter nötig die ist.

Bei Vorlage eines Papiers bestätigte der stellvertretende Pentagon Chef William Lynn, dass die Behörde im März Opfer eines der größten Hackerangriffe ihrer Geschichte geworden ist. 24 000 sensible Dokumente seien in die Hände von ausländischen Eindringlingen in das Netzwerk einer Vertragsfirma gelangt. Allein beim US-Militär müssten 15 000 Netzwerke und rund sieben Millionen Computer vor millionenfachen Hackerangriffen pro Tag beschützt werden, sagte Lynn. „Die Cyberbedrohung ist akut und potenziell verheerend. Gegner suchen konstant nach Schwachstellen." Pro Jahr würden so viele Informationen von den Festplatten amerikanischer Unternehmen, Universitäten und Behörden gestohlen, wie die Kongressbibliothek in Washington fasst. Dort stehen 147 Millionen Datenträger - davon allein 33 Millionen Bücher. Täglich würden mehr als 60 000 neue Computerschädlinge als Bedrohung identifiziert.

Weiter wird berichtet und bestätigt von Sony, Gema und selbst der CIA.

Die Zahl der Hackerangriffe wächst kontinuierlich

und die Schwere und Dauer nimmt dabei zu!

Weitere Nachrichten vom 26.12.2011 aus Fenancee.de

Die Hacker-Organisation "Anonymous" hat nach eigenen Angaben sensible Daten wie Email-Adressen und Kreditkartennummern von tausenden Kunden der US-Sicherheitsfirma Stratfor geknackt. Die Gruppe veröffentlichte am Sonntag im Kurznachrichtendienst Twitter einen Internet-Link zu einer angeblichen Liste von Stratfor-Kunden. Stratfor räumte einen Hackerangriff ein.

Unter den Kunden, deren Daten veröffentlicht wurden, sollen sich nach Angaben der Hacker das US-Verteidigungsministerium, die US-Armee, die US-Luftwaffe und Technologie-Giganten wie Apple und Microsoft befinden. Ein mutmaßlicher Anonymous-Hacker vermeldete über Twitter, die Zugangsdaten für 90.000 Kreditkarten seien geknackt worden. Damit sei es möglich gewesen, von diesen Karten unfreiwillige Spenden im Gesamtumfang von mehr als einer Million Dollar (rund 770.000 Euro) abzubuchen.

Unter den genannten Beispielen war eine 494-Dollar-Spende an die Hilfsorganisation CARE von Seiten des US-Verteidigungsministeriums und eine 180-Dollar-Spende von einem Mitarbeiter des Heimatschutz-Ministeriums an das Rote Kreuz.

Die US-Sicherheitsfirma Stratfor hat eingestanden, Kreditkartendaten und persönlichen Informationen seiner Kunden nicht verschlüsselt zu haben. Die Hackergruppe Anonymous, die sich zum Cyberangriff auf Stratfor bekannte, hatte die Daten inklusive Kreditkarteninformationen von über 75'000 Kunden veröffentlicht, darunter auch von Schweizer Behörden und Unternehmen.

Als schweren Hackerangriff bezeichnet man also, wenn wirklich sensible Daten gestohlen werden und mit diesen dann noch Schindluder betrieben wird. Industriespionage, beispielsweise bei Rüstungskonzernen zählt ebenfalls zu dieser Kategorie. Oder aber neuartige Technologie ausspionieren oder gar stehlen. Sensible Daten sind jedoch überall zu finden, denken Sie z.B. an diverse Kundendaten. Ein Unternehmen, was brisante Kundendaten beherbergt, **hat besondere Schutzmaßnahmen zu treffen**.

Weiterer Bericht: Hackergruppe *Lizard Squad* nutzt gekaperte Heimrouter für DDoS-Angriffe

Den Artikel dazu lesen Sie hier.

Was ist ein Penetrationstest?

Ein Penetrationstest ist der Prozess, Angriffe auf ein Netzwerk und die zugehörigen Systeme zu simulieren. Er dient zur Abschätzung der Erfolgsaussichten eines Angriffs. In einem solchen Test wird das Angriffsverhalten eines vorsätzlichen Innen- oder Außentäters (Studien zufolge kommen 30 Prozent der Täter von außen und 70 Prozent von innen) simuliert, wobei das Ziel zu verfolgen ist, evtl. Schwachstellen zu finden und des daraus resultierenden tatsächlichen Schutzes sowie die Meldung und Erkennung verdächtiger Aktivitäten (IDS = Intrusion Detection System, z.B. SNORT) und welche potentiellen Schäden durch einen Angriff entstehen können.

Diese Simulationen erfordert unbedingt die Zustimmung des Auftraggebers oder des Eigentümers.

Penetrationstests werden über das Ziel und das Ausmaß der Prüfungsabhandlungen genau dokumentiert, auch über mögliche Ausfälle und Risiken, die durch den Test entstehen können werden hier festgehalten.

Bei einer Simulation eines Innentäters wird meist der Ansatz eines White-Box Test verfolgt. Das heißt, es wird davon ausgegangen, dass der Angreifer über detaillierte Kenntnisse über die innere Struktur der Anwendungen und Dienst verfügt. Demgegenüber steht der Blackbox Test[2], der meist auf den Ansatz eines Angreifers von außen angewandt wird.

Nachdem eine ausführliche Dokumentation über die Vorgehensweise vorliegt, läuft der eigentliche Test folgendermaßen ab (er wird in fünf Schritten beschrieben):

Aufdeckung (discovery) – Recherche von frei zugänglichen Informationen über das Ziel oder den Untersuchungsgegenstand, z.B. der IP-Adressen.

Enumeration (Auflistung, Aufzählung) – Mittels Portscanner wie NMap oder ähnlichen Analysetools werden die vom Zielsystem angebotenen Dienste oder die evtl. geöffneten Ports ermittelt. Auf die evtl. geöffneten Ports können sodann Rückschlüsse gezogen werden welche Anwendungen und Dienste zur Verfügung stehen, bzw. für einen Angriff genutzt werden können.

Schwachstellenanalyse (vulnerability mapping) – Identifikation der Schwachstellen der Systeme bzw. welche Ressourcen auf dem Zielsystem vorhanden sind.

Ausnutzung (exploitation) – Versuchen, sich unter Ausnutzung der Schwachstellen unberechtigten Zugang zu verschaffen.

Berichterstattung – Dokumentation der Prüfungsfeststellungen und möglicher Gegenmaßnahmen. Der Bericht ist auch der Geschäftsführung mitzuteilen.

Neben den Begriffen WhiteBox-Test und BlackBox-Test gibt es noch einen weiteren Wissensstand zur Durchführung eines Penetrationstests. Zum Schema fehlt noch der GreyBox-Test.

Blindtest (zero-knowledge, Blackbox-Test oder BlackBox-Ansatz) – Der Penetrationstester hat keinerlei Informationen über das Ziel und muss entsprechend vorgehen.

Teilinformationen (Greybox-Test) – Der Penetrationstester hat ausgewählte Informationen über das Ziel.

Vollinformation (WhiteBox-Test oder WhiteBox-Ansatz) – Alle Informationen über das Ziel liegen vor und der Penetrationstester kann entsprechend den Informationen vorgehen.

Es ist wichtig, das der Penetrationstester mit einfachen Angriffen beginnt, um wirklichkeitsgetreue Angriffe zu simulieren, die denen eines gewöhnlichen Anwenders entspricht. Der Penetrationstester muss eine Vielzahl von Werkzeugen und Angriffsmethoden einsetzen, um alle möglichen Schwachstellen zu untersuchen, da dies dem wirklichen Vorgehen eines Angreifers entspricht und er keine Versuche auslassen wird, bis er sein Ziel erreicht hat. ***Wichtig zu wissen ist demnach auch, wie die Motive eines Angreifers sein können.***

Motive können sein, Rache (auch von ausgeschiedenen Mitarbeitern), Geltungssucht, Furcht, das Robin-Hood-Motiv, Materielle Interessen, Neugierde usw. Ein Penetrationstester sollte in der Lage sein, sich in einen Angreifer hineinversetzen zu können, nur so ist gewährleistet, dass ein Penetrationstest wirklichkeitsgetreu ablaufen kann.

Kenne Deinen Feind,
denn er ist der Schlüssel zum Erfolg.

In Punkt **„Ausnutzung der Schwachstellen“** ist nicht unproblematisch zu betrachten, da durch diese Test evtl. der produktive Betrieb gestört werden kann oder im schlimmsten Fall neue Schwachstellen hinzukommen könnten. Auch besteht die Möglichkeit, dass Daten Manipuliert werden und diese vorher in Sicherungskopie hinterlegt sein sollten. Auch Datenschutzrechtliche Belange sind mit einem Penetrationstest verbunden und dürfen so nur in Absprache mit dem Betreiber und Datenschutzbeauftragten durchgeführt werden.

Zum Schluss ist anzumerken, dass ein Penetrationstest für ein Unternehmen sich positiv auswirken kann (z.B. für den Datenschutz, für den jedes Unternehmen verpflichtet ist, diesen Einzuhalten), da ein solcher Test vor vielen Gefahren schützen kann, jedoch ist es unerlässlich, dass diese Tests von Fall zu Fall, bzw. nach einiger Zeit wiederholt werden sollten, da täglich neue Schwachstellen in Betriebssystemen und Anwendungen entstehen.

Penetrationstest gehören heute zum festen Bestandteil für Dienstleistungen im Sicherheitssektor. Sie versprechen mehr Sicherheit durch die Prüfung von IT-Infrastrukturen. Oft wird jedoch das Wort "Penetrationstest" marketingtechnisch verwendet. Ein echter Penetrationstester nimmt kaum Rücksicht auf die vorhandene Hard- und Software sowie deren Prozesse, die ein Cracker anwenden würde, um Kontrolle über ein System zu erlangen. Deshalb verwenden wir in unserer Dienstleistung nicht das Wort "Penetrationstest". Wir gehen auch nicht mit der Gewalt eines Crackers vor, sondern wir arbeiten hier mit "Sicherheitstests", die jedoch mit denselben Werkzeugen bestritten werden können.

Die aufgeführten Punkte sind des Verständnisses wegen einfach gehalten worden und enthalten keine Anleitungen sowie anderweitig nutzbare Auszüge und verwertbarem zu möglichen Angriff Szenarien zu nutzen oder auszunutzen.

Warum eine Allianz wichtig ist!

Das bisherige Dokument verdeutlicht die Thematik der Vergangenheit und lässt und in Zukunft nur erahnen, mit welchen Mitteln Kriminelle auf der Suche nach neuen Exploits sind und lässt nur einen vernünftigen Schluss zu, dass die Industrie, Dienstleister, öffentliche Bereiche und der Bankensektor genauso zusammenarbeiten müssen, wie es die Betrüger, Hacker und deren Motive tuen.

Cyber-Attacken nehmen kontinuierlich zu und haben auch im vergangenen Jahr stark zugenommen. Nur mit vereinten Kräften, ist es möglich den Angriffen zu begegnen und Schäden effektiv zu minimieren.

Die kommenden Cyber-Attacken 2015

Im Jahr 2014 hat die Cyberkriminalität weiter an Dynamik gewonnen. Die massenhaften Kompromittierungen von Wordpress und die Spear-Phishing-Attacke auf das Weiße Haus sind dafür nur zwei der prominentesten Beispiele. Damit Unternehmen im Jahr 2013 gut gerüstet sind, prognostizieren die Websense Security Labs die sieben größten Bedrohungen für das nächste Jahr.

Damit Unternehmen im Jahr 2013 gut gerüstet sind, prognostizieren die Websense Security Labs die sieben größten Bedrohungen für das nächste Jahr.

Vor allem mobile Computer werden zukünftig im Fokus von Würmern, Viren, Trojanern und Hackern stehen.

Das letzte Jahr hat Attacken und Exploits gesehen, die unsere Vorstellung von **Kriminalität**, **Wirtschaftsspionage** und **Kriegsführung** neu definiert haben. Das Jahr 2013 wird weiter verdeutlichen, dass sich die fortgeschrittenen Cyber-Attacken mit herkömmlichen Sicherheitsmaßnahmen nicht länger effektiv bekämpfen lassen", sagt Michael Rudrich, Regional Director Central Europe bei Websense in München.

"Unternehmen und Anbieter von Sicherheitslösungen müssen viel mehr auf proaktive Echtzeit-Abwehr setzen."

Die 7 grössten Bedrohungen für das Jahr 2013 waren:

1. Mobile Geräte sind das Ziel

Cyber Kriminelle werden die drei mobilen Plattformen Windows 8, Android und iOS verstärkt ins Visier nehmen. Webbasierte plattformübergreifende Exploits erleichtern den Tätern dabei die Attacken. Am stärksten zunehmen werden die Bedrohungen für Microsoft-Mobilgeräte. Um an Nutzerberechtigungen für Mobilgeräte zu gelangen, werden die Angreifer immer häufiger auf Social-Engineering-Methoden als Köder setzen.

2. Bypass-Methoden umgehen Sandbox-Erkennung

Viele Unternehmen nutzen virtuelle Maschinen für Tests auf Schadsoftware. Deshalb entwickeln die Angreifer Methoden, die virtuelle Umgebungen als solche erkennen. Einige davon werden versuchen, eine Sicherheits-Sandbox zu identifizieren – und zwar genau so, wie in der Vergangenheit bestimmte Antivirenmaschinen angegriffen und ausgeschaltet wurden. Diese fortgeschrittenen Attacken werden sich so lange verbergen, bis sie sicher sind, nicht in einer virtuellen Sicherheitsumgebung zu sein.

3. Legale App-Stores beherbergen mehr Schadsoftware

Bösartige Apps werden im Jahr 2013 immer häufiger unerkannt durch die Prüfungsprozesse schlüpfen und dadurch eine immer größere Bedrohung für Unternehmen mit BYOD-Strategie (Bring Your Own Device) darstellen. Da immer mehr Betriebe BYOD erlauben, werden außerdem auch die Gefahren durch freigeschaltete ("jail broken") und gerootete Geräte sowie unautorisierte App-Stores wachsen.

4. Staatlich geförderte Attacken steigen

Mehr Regierungen werden in den Cyberkrieg eintreten. Die öffentlich gewordenen Attacken animieren Nachahmer, weitere Faktoren werden diesen Trend verstärken: Während es für die meisten Länder unerreichbar scheint, eine Atommacht zu werden, können praktisch alle das Talent und die Ressourcen heranziehen, die es für Cyberwaffen braucht. Außerdem haben die Länder und die entsprechenden Personen problemlos Zugang zu Vorlagen aus vergangenen Angriffen wie Stuxnet, Flame und Shamoon.

5. "Hacktivisten" erreichen nächstes Level

Hacktivist > siehe Motive = moderner Robin Hood.

Die Angriffe durch so genannte Hacktivisten, politisch motivierte Hacker, waren in der Vergangenheit äußerst öffentlichkeitswirksam. Deshalb haben sich die Unternehmen auf derartige Bedrohungen eingestellt und immer besser funktionierende Strategien und Lösungen umgesetzt. Die Hacktivisten werden darum ihre Methoden weiter verfeinern und dabei im Jahr 2013 den nächsten Level erreichen.

6. Schadhafte E-Mails feiern Comeback

Gezielte und genau getimte Spear-Phishing-Attacken, vermehrte bösartige Anhänge: Schadhafte E-Mails feiern 2013 ein Comeback. Mit Methoden wie DGA (Domain Generation Algorithmus), welche die Herkunft der Mails verschleiern, werden die Angreifer die gängigen Schutzmaßnahmen aushebeln.

7. Cyberkriminelle greifen Content-Management-Systeme an

In der Vergangenheit wurden Schwachstellen in Wordpress regelmäßig für massenhafte Manipulationen genutzt. Derzeit gewinnen andere Content-Management-Systeme und Service-Plattformen im Web zunehmend an Popularität. Cyberkriminelle werden die Integrität dieser Systeme regelmäßig testen. Auch weiterhin werden es seriöse Plattformen sein, die von Angriffen betroffen sind. Sie werden mit dem Ziel attackiert, Malware einzuschleusen, Nutzer zu infizieren und in Unternehmen einzudringen, um deren Daten zu stehlen. CMS-Administratoren müssen deshalb Updates, Patches und anderen Sicherheitsmaßnahmen mehr Beachtung schenken.

Die 8 grössten Cyber-Attacken 2015

Aufgestellt von Security-Software-Hersteller ESET.

1. Cyber-Attacken dauern immer länger

Mittlerweile dauern die meisten Angriffe mehrere Wochen an. Die 2014 im Radware-Bericht am häufigsten genannte Angriffsdauer war ein Monat. Zugleich waren 19 Prozent der größten Angriffe als dauerhaft zu bezeichnen. Diese Befunde stehen in starkem Kontrast zur Sicherheitslage in den vergangenen Jahren, in denen nie mehr als sechs Prozent der verzeichneten Angriffe als lang anhaltend eingestuft wurden. Die zunehmende Dauer und Stärke der Attacken stellt vor allem deshalb eine große Gefahr dar, da die meisten Unternehmen und Organisationen darauf nicht vorbereitet sind. So können derzeit 52 Prozent der Unternehmen ihre Abwehr nur einen Tag lang oder sogar noch kürzer aufrechterhalten.

2. Regierungen, Gaming- und Internet-Serviceanbieter besonders im Visier

Besonders im Fokus von Cyber-Attacken stehen derzeit wie auch schon in den Vorjahren Regierungsorganisationen und Internet-Serviceanbieter. Neu im Kreis der am stärksten gefährdeten Branchen ist die Gaming-Industrie, die schon 2014 von zahlreichen spektakulären und wiederholten Angriffswellen betroffen war. Eine leichte Entspannung ist hingegen bei Banken und Versicherungen eingetreten, die vor allem 2012 und 2013 Opfer heftiger und vor allem politisch motivierter Angriffe waren.

3. DDoS-Attacken nutzen neue Schwachstellen

In den vergangenen Jahren richteten sich DDoS(Distributed Denial of Service)-Attacken vor allem gegen Server oder Firewalls. Mittlerweile ist jedoch der Internetzugang zur Schwachstelle Nummer eins geworden. Grund dafür war vor allem ein Anstieg von UDP(User Datagram Protocol)-Attacken.

4. DDoS-Attacken sind fast immer Mehrfachangriffe

2015 wird endgültig die übergroße Mehrheit der DDoS-Attacken mehrere Angriffsmethoden gleichzeitig einsetzen, um die Verteidigungslinien zu durchbrechen. Zu diesem Methodenmix gehören vor allem die Anonymisierung, Maskierung und Fragmentierung bösartiger Datenpakete, der Einsatz dynamischer Parameter, Umgehungs- und Kodierungstechniken, sogenannte Parameter Pollution und der extensive Missbrauch von Anwendungsfunktionen.

5. Cloud Computing und Internet der Dinge schaffen neue Sicherheitslücken

2015 werden neue Sicherheitslücken für Schlagzeilen sorgen, die Folge davon sind, dass sich die klassischen IT-Netzwerke der Unternehmen auflösen. So ist der Trend zum Cloud Computing ungebrochen, das „Internet der Dinge" ist auf dem Vormarsch, und die traditionellen auf Hardware basierten Netzwerke werden zunehmend durch „Software Defined Networks" abgelöst. Diese Trends stellen IT-Sicherheitsteams vor völlig neue Herausforderungen, da die Abwehr von Angreifern auf einer wesentlich breiteren Front stattfinden muss. 2015 ist davon auszugehen, dass Hacker die bei diesen Umbrüchen auftretenden Schwachstellen gezielt ausnutzen werden.

ESET zufolge rangiert 2015 an erster Stelle der Gefahren:

1. Das „Internet der Dinge" – ein neues Spielzeug für Hacker

Immer mehr Geräte sind mit dem Internet verbunden. Die Informationen, die sie speichern, werden im neuen Jahr ein interessantes Ziel für Hacker. Bereits 2014 zeigten sich die ersten Hinweise für einen wachsenden Trend unter Cyberkriminellen in diesem Bereich. Wie vielseitig diese Attacken sind, wurde auf der „Defcon Hacking Conference" in diesem Jahr deutlich, als ein Auto von Tesla über die Steuereinheit des Motors zum Öffnen der Türen gebracht wurde. Ebenfalls gehackt wurden verschiedene Smart TVs, „Boxee" Streaming-Boxen, biometrische Systeme auf Smartphones, Router sowie die Datenbrille „Google Glass".

2. Digitale Bezahlsysteme ziehen Malware magisch an

Nachdem digitale Bezahlsysteme immer mehr Anklang bei den Nutzern finden, steigt auch das Interesse bei Malware-Autoren, die sich durch ihre Attacken finanziell bereichern möchten. 2014 wurde die bisher größte Attacke auf ein digitales Bezahlsystem verzeichnet, bei dem Hacker über 600.000 US-Dollar in Bitcoins und Dogecoins erbeutet haben. Für ihre Attacke verwendeten sie ein Netzwerk infizierter Maschinen.

3. Gezielte Angriffe nehmen zu

Ein ähnlich aggressives Vorgehen zeigt sich auch bei gezielten Angriffen, die bereits 2014 für Unruhe sorgten. Diese Art von Cyberattacken unterscheidet sich von klassischen Angriffen und zielt auf ausgewählte Opfer ab. 2015 werden solcherlei Attacken nach Einstätzung der ESET-Sicherheitsexperten noch raffinierter. „Die Hacker machen sich hierbei häufig ‚Social Engineering' zu Nutze", erklärt Pablo Ramos, Head of Research Lab bei ESET Lateinamerika. "Dabei spionieren die Hacker das soziale Umfeld der potentiellen Opfer aus, täuschen Identitäten vor oder nutzen Verhaltensweisen aus, um die Opfer dazu zu bringen bestimmte Handlungen auszuführen oder vertrauliche Informationen preiszugeben."

Die 7 grössten Cyber-Attacken 2016

1. Cyber-Erpressung

Dabei wird die Psychologie der Angriffsstrategie eine deutlich größere Rolle spielen als die technischen Auswirkungen, denn aus Sicht der Hacker hat es sich als sehr effektiv erwiesen, ihren Opfern Furcht einzujagen. Sie haben in den zurückliegenden zehn Jahren Lösegeld mithilfe von Software erpresst. Mithilfe von abgefangener Kommunikation zwischen Geschäftspartnern sollen Unternehmen dazu gebracht werden, Geld zu überweisen.

2. Hacktivisten sind auf dem Vormarsch

Zielpersonen sollen möglichst Publikumswirksam Rufgeschädigt werden. Bekannte Firmen werden die Auswirkungen der dadurch verursachten Datenschäden zu spüren bekommen. Hacktivisten werden, wenn sie bislang vor allem Standardtaktiken wie DDoS-Angriffe oder die Verunstaltung von Websites eingesetzt haben, nun nach Verfahren suchen, Datenlecks auszunutzen oder zu verursachen.

3. Das Internet der Dinge gerät unter Beschuss

Immer mehr Mobile Geräte befinden sich im Netz. Bis 2019 wird erwartet, dass 2 Milliarden Geräte vernetzt sein werden. In diesem Jahr können auf smarten Geräten Fehlfunktionen katastrophale Folgen haben. Das können sein, gehackte Baby Fons, TV-Geräte oder auch Autos.

4. Unvorsichtige Firmen

Bis Ende 2016 werden weniger als 40 % aller Unternehmen Experten beschäftigen, die auf Cybersicherheit spezialisiert sind. Zwar werden einige dieser Firmen erkennen, dass Angestellte vonnöten sind, deren Augenmerk einzig und allein auf der Sicherheit von Daten innerhalb und außerhalb des eigenen Betriebs liegt. Jedoch hängt dies von Faktoren ab, wie zum Beispiel dem Budget oder der Größe des Unternehmens sowie Fehlens des grundlegenden Verständnisses.

5. schädliche Online Werbung

In diesem Jahr werden vorzugsweise Exploit-Kits verwendet, die auf Schwachstellen von Adobe Flash angesetzt werden sowie vermehrt auf Zero-Day-Exploit. Die Industrie und Hersteller sind teilweise diesem Ansturm hoffnungslos ausgesetzt.

6. Mobile Angriffe

Bis zu 20 Millionen Angriffe werden in diesem Jahr erwartet, wovon vor allem China betroffen sein wird. Während Google bekannt gegeben hat, dass der Play Store weniger als ein Prozent der Apps potenziell gefährlich sind, sind es in China 13 Prozent.

7. Cyber-Straftaten

Im Bereich der Gesetzgebung soll es, um den Aktivitäten der Cyberkriminellen begegnen zu können, im Jahr 2016 konkrete Veränderungen - bis hin zu weltweiten Anstrengungen - geben. Diese sollten zu einer schnelleren Ausführung, mehr Verurteilungen, Verhaftungen und erfolgreicheren Strafverfahren führen.

Aus diesen Gründen ist es wichtig, sich einer Allianz anzuschließen, um gemeinsam nach Lösungen zu suchen.

Allianzen, denen Sie sich anschließen können:

Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik und des Vereins BITKOM.

https://www.allianz-fuer-cybersicherheit.de/ | Deutschland

In der Melde- und Analysestelle Informationssicherung MELANI arbeiten Partner zusammen, welche im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen kritischen Infrastrukturen tätig sind.

Melde- und Analysestelle Informationssicherung MELANI | Schweiz

Dies ist ein Whitepaper von

Mail: info@netSecure-IT.de
Internet: http://netSecure-IT.de