Phishing und Pharming: Diebstahl im Netz

Phishing (fish'ing) n. - *Eine Methode, bei der mit Hilfe so genannter Spoof-Mails, die aus vertrauenswürdigen Quellen zu stammen scheinen, persönliche Daten gestohlen werden.*

Pharming (farm'ing) n. - *Eine Methode, bei der Internetverkehr über Domain-Spoofing zu einer gefälschten Website umgeleitet wird.*

Ganz gleich, ob Sie nur gelegentlich im Internet surfen oder geradezu online leben, als Internetnutzer unterliegen Sie stets der Gefahr eines Angriffs durch Phishing-E-Mails, Pharming-Seiten und Crimeware. Da Internetkriminelle immer häufiger Botnets (Netzwerke von manipulierten PCs) nutzen, um nicht verfolgbare, Spam-basierte Phishing-Angriffe zu starten, ist die Zahl der Phishing- und Pharming-Methoden drastisch gestiegen. Kriminelle arbeiten mit komplexen oder vielschichtigen Angriffsmethoden, die verschiedene Crimeware-Techniken kombinieren, um Identitäten zu stehlen und Systeme zu kidnappen, und tricksen dabei oft auch versierte Benutzer aus.

Der Finanzsektor ist mit Abstand das größte Ziel von Angriffen. So erstellen Internetbetrüger häufig gefälschte Websites, die das Aussehen legaler Bank- und Börsenseiten genau imitieren, um Benutzer dazu zu bringen, ihre Online-Kontonamen, Kennwörter, Sozialversicherungsnummern und andere persönliche Daten auszuhändigen.

Phishing-Tricks

Durch Spam oder gezielte E-Mails versuchen Phisher, Benutzer auf gefälschte Websites zu locken. Dies geschieht in der Hoffnung, tatsächliche Kunden der betroffenen Banken, Kreditkartenfirmen oder Internethändler zu finden. Derartige E-Mails können äußerst überzeugend erscheinen, so wie beispielsweise eine Nachricht von eBay mit dem Inhalt, dass die Kreditkarte abgelehnt wurde, oder der Citibank, dass nicht autorisierte Aktivitäten auf dem Konto festgestellt wurden. Die Nachrichten enthalten häufig Logos, Farbschemas und Firmenslogans ("Avis: We Try Harder"), die echt erscheinen.

Ein weiteres Beispiel ist eine Spam-Mail, die angeblich von BBC News versendet wurde. Die E-Mail enthielt den Anfang einer interessanten Pressemitteilung sowie einen Link "Vollständiger Artikel", um Benutzer auf eine gefälschte BBC News-Seite umzuleiten. Die gefälschte Website sah exakt so aus wie die echte BBC News-Website und enthielt echte Pressemitteilungen, die von der BBC-Seite kopiert worden waren. Die gefälschten Webseiten hatten die nicht gepatchte Sicherheitslücke "Textbereich erstellen" ausgenutzt, um einen Keylogger herunterzuladen und zu installieren. Mit diesem Keylogger wurden die Aktivitäten von Benutzern auf verschiedenen Finanzseiten überwacht und die aufgezeichneten Daten zurück zum Hacker gesendet.

Pharming-Techniken

Beim Pharming wird die Technik des DNS (Domain Name Service)-Hijacking oder -Poisoning verwendet. Benutzer werden zu einer gefälschten Website umgeleitet, indem die DNS für die Zielwebsite geändert wird. Oder das System leitet Benutzer über von Phishern gesteuerte Proxies, die dazu genutzt werden können, Tastatureingaben zu überwachen und abzufangen, zu echten Websites um.

Die manipulierten Websites sammeln Kreditkartennummern, Kontonamen, Kennwörter und Sozialversicherungsnummern. Dies geschieht entweder durch Anzeigen eines Popups, um die entsprechenden Daten zu stehlen, bevor der Benutzer zu der echten Website weitergeleitet wird, oder durch die Verwendung eines selbstsignierten Zertifikats, um eine Authentifizierung vorzutäuschen und den Benutzer dazu zu bringen, persönliche Daten auf der manipulierten Website einzugeben, oder aber durch Überschreiben der Adresse und der Statusleiste des Browsers, um den Benutzer glauben zu lassen, er befände sich auf der legalen Website, so dass er seine Daten eingibt.

Crimeware: Manipulierte Downloads

Mit Hilfe von Tricks installieren Phisher Crimeware auf den Computern von Benutzern, um vertrauliche Informationen direkt stehlen zu können. In den meisten Fällen merkt der Benutzer nicht, dass sein System infiziert wurde, sondern stellt nur eine leichte Einschränkung der Computerleistung oder kurze Betriebsstörungen fest, die auf normale Softwareausfälle zurückgeführt werden. Sicherheitssoftware ist ein unerlässliches Tool, um die Installation von Crimeware zu verhindern, wenn Sie von einem Angriff betroffen sind.

Bei einem manipulierten Download werden Trojaner, Keylogger und andere Spyware-Programme zusammen mit legaler Software heruntergeladen, oder der Hacker modifiziert eine seriöse Seite mit Hilfe schädlicher Skripts, so dass die Software im Hintergrund heruntergeladen wird, wenn der Benutzer auf eine vertrauenswürdige Website zugreift. Auch mit Social Engineering-Techniken versuchen Phisher, Benutzer dazu zu verleiten, die Software direkt von ihrer Seite herunterzuladen, indem sie ihnen diese, z.B. als Bildschirmschoner oder Programme zum Herunterladen von Musik, schmackhaft machen.

Hat sich Crimeware erst einmal auf Ihrem System installiert, stecken Sie in Schwierigkeiten. Crimeware kann dazu führen, dass der Browser Spoof-Seiten startet oder dass die Hostdatei des PCs dazu missbraucht wird, den Computer auf Spoof-Seiten umzuleiten. Crimeware kann außerdem Keylogger und Screen-Scraper dazu verwenden, gestohlene Daten aufzuzeichnen und zurück zum Hacker zu senden. Darüber hinaus installiert Crimeware Rootkits, die versteckt arbeiten und die Existenz von Spyware verbergen, oder integriert den PC in ein ferngesteuertes Botnet, über das Massenspam- oder Denial-of-Service-Angriffe gestartet werden können.

Phishing-Trends

Aktuellen Informationen zufolge nehmen Phishing-Angriffe rasant zu. Zehntausende von speziellen Phishing-Fällen werden jedes Jahr gemeldet, und diese Zahlen steigen überproportional an. Ein ähnlicher Anstieg ist für neue Phishing-Seiten zu verzeichnen, ebenso wie für Websites, die bösartigen Code zum Stehlen von Kennwörtern enthalten. Die meisten Phishing-Seiten sind in den USA gehostet, gefolgt von China und Korea.

Dabei richten Phisher ihre Angriffe zunehmend gegen große Finanz- und E-Commerce-Unternehmen. So waren beispielsweise von 100 betroffenen Firmen ca. 5 Opfer von 80 % der gesamten Phishing-Kampagnen. Da eBay und große Finanzinstitute verstärkt präventive Maßnahmen zur Bekämpfung von Phishing ergreifen, konzentrieren Kriminelle sich mehr und mehr auf kleinere Kreditunternehmen und weniger geschützte Firmen. Aufgrund des geschärften Bewusstseins der Benutzer für die Gefahren durch Phishing-Angriffe treten diese seltener in Form von Spam auf, sondern nutzen stattdessen verstärkt Sicherheitslücken aus.

Die 10 besten Tipps zum Schutz vor Phishing

1. **Aktualisieren Sie Ihr Betriebssystem stets mit den neuesten Patches, um das Ausnutzen bekannter Software-Sicherheitslücken zu vermeiden.** Installieren Sie Patches von Software-Herstellern, sobald diese veröffentlicht werden, da Hacker in der Lage sind, innerhalb kürzester Zeit aus bereits zuvor entwickelten Komponenten Malware zu erstellen, um die Schwachstelle auszunutzen, bevor die Mehrheit der Benutzer den Patch heruntergeladen hat. Ein mit sämtlichen Patches versehener Computer hinter einer Firewall ist die beste Verteidigung gegen Trojaner- und Spyware-Installationen.

2. **Laden Sie die neueste Version Ihres Browsers herunter, um zu gewährleisten, dass dieser auf dem neuesten Stand ist und aktuelle Technologien nutzt.** Internet Explorer 7 und andere Browser beinhalten als zusätzliche Sicherheitsstufe eine Antiphishing-Symbolleiste.

3. **Die Herkunft einer E-Mail, die Adresse einer Website und die verwendete SSL-Verschlüsselung können gefälscht sein.** Das in der Statusleiste des Browsers angezeigte Sperrsymbol kann ebenfalls gefälscht sein. Stellen Sie sicher, dass eine SSL-Verschlüsselung verwendet wird (achten Sie auf "https:" in der URL) und überprüfen Sie den Domainnamen der Seite als Indikator dafür, ob es sich um eine legale Seite handelt. Da Hacker mit immer neuen Tricks arbeiten, können Sie sich nicht allein auf diese Überprüfungen verlassen, um die Sicherheit einer Verbindung oder Website zu garantieren.

4. **Klicken Sie nie auf einen Link in einer unverlangt zugesandten E-Mail und ignorieren Sie E-Mails, die eine Handlungsaufforderung beinhalten, wie z.B. "Ihr Konto wird deaktiviert."** Fragen Sie stattdessen telefonisch bei der Firma nach und verwenden Sie dazu eine andere als in der E-Mail angegebene Telefonnummer.

5. **Seien Sie äußerst vorsichtig, wenn Sie Software aus dem Internet herunterladen.** Zusammen mit der legalen Software kann Spyware heruntergeladen werden, oder die Software enthält Keylogger oder Screen-Scraper, die ihre persönlichen Daten erfassen. Sie sollten generell keine kostenlosen Bildschirmschoner oder anderen Gratisangebote herunterladen. Seien Sie außerdem vorsichtig beim Öffnen von E-Mail-Anhängen, z.B. Videos, Grafiken oder PDFs, auch wenn diese von bekannten Personen kommen. Virenschutzsoftware schützt Sie, indem bereits vor dem Öffnen des Anhangs festgestellt wird, ob sich Viren darin verbergen.

6. **Verwenden Sie Software, die automatisch überprüft, ob eine URL legal ist, bevor Sie auf die Seite geleitet werden.** Testen Sie AccountGuard von eBay und ScamBlocker von EarthLink Sie können die Authentizität einzelner Internetadressen (URLs) darüber hinaus mit einer „Wer ist“-Suche, z.B. über www.DNSstuff.com, überprüfen. Die Seite beinhaltet eine Suchfunktion, über die die Kontaktdaten für eine Domain/IP-Adresse in fast allen Ländern angezeigt werden können.

7. **Wählen Sie einen Internet Service Provider (ISP), der leistungsstarke Antispam- und Antiphishing-Technologien und -Richtlinien einsetzt.** AOL beispielsweise blockiert bekannte Phishing-Seiten, so dass Kunden nicht darauf zugreifen können. Die Organisation SpamHaus führt die 10 derzeit schlechtesten ISPs in dieser Kategorie auf. Berücksichtigen Sie diese Liste bei Ihrer Wahl.

8. **Überprüfen Sie Kreditkarten- und Kontoauszüge unverzüglich nach deren Erhalt, um unberechtigte Abbuchungen auszuschließen**. Wenn Ihr Auszug bereits seit mehreren Tagen fällig ist, rufen Sie Ihr Kreditkartenunternehmen oder Ihre Bank an, um Ihre Rechnungsadresse und Ihren Kontostand zu bestätigen.

9. **Übernehmen Sie frühzeitig neue Technologien.** Banken und Kreditkartenunternehmen verwenden neue Validierungstechniken, um Online-Transaktionen sicherer zu machen, also nutzen auch Sie diese Techniken. Die Computerindustrie arbeitet zudem an Authentifizierungstechnologien, wie z.B. Sender-ID, Domainname und S/MIME, die die Auswirkungen von Phishing-Angriffen minimieren sollen.

10. **Schützen Sie Ihren Computer mit zuverlässiger Sicherheitssoftware und stellen Sie sicher, dass ihr Schutz immer auf dem neuesten Stand ist.** Hacker verfügen über Datenbanken, die Millionen von E-Mail-Adressen enthalten. Sie zielen auf Sicherheitslücken in E-Mail-Anwendungen und Internetbrowsern ab und missbrauchen Design-Schwachstellen in ausgewählten Website-Programmen. Dennoch können Sie sich vor Phishing-Angriffen schützen, die herkömmliche Spam-Techniken und Methoden zur Ausnutzung von Softwareschwachstellen kombinieren.

    McAfee Internet Security Suite garantiert zuverlässigen Schutz Ihres PCs vor Viren, Hackern und Spyware. Zu den einzigartigen Features der Lösung gehört X-Ray für Windows, das Rootkits und andere bösartige Anwendungen, die sich vor Windows und anderen Virenschutzprogrammen verbergen können, erkennt und löscht. Die integrierten Antiviren-, Antispyware-, Firewall-, Antispam-, Antiphishing- und Backup-Technologien greifen zum Schutz vor den heutigen hochentwickelten und komplexen Bedrohungen nahtlos ineinander.

McAfee GmbH
Ohmstr. 1
85716 Unterschleissheim
+49-89-3707 0
www.mcafee.de