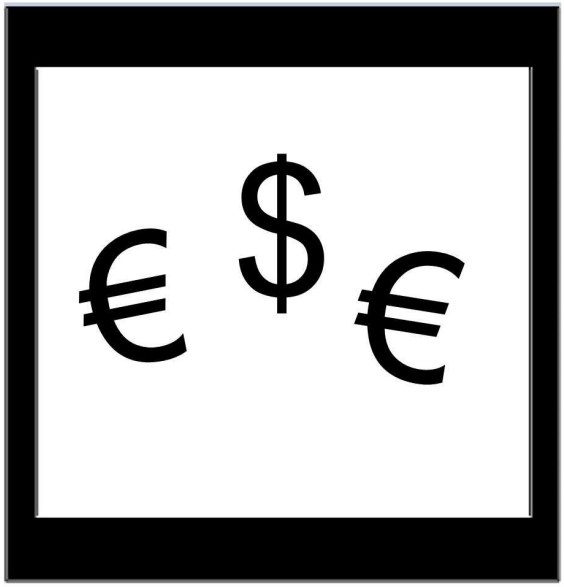
POLIZEI
Nordrhein-Westfalen
Kreis Warendorf

bürgerorientiert · professionell · rechtsstaatlich



Kreispolizeibehörde Warendorf
Sicheres Online-Banking

Eine Kurzanalyse zu den Risiken des gebräuchlichsten Online-Banking mittels Windows-PC und Standard-Browser, sowie verschiedene Lösungsansätze.

Impressum:

Herausgeber: Der Landrat als Kreispolizeibehörde Warendorf
Waldenburger Straße 2 – 4, 48231 Warendorf
Redaktion: Kriminalkommissariat 1
Realisierung und redaktionelle Bearbeitung: KHK Martin Habrock

Oktober 2015

1 Vorwort

Seit mehr als vier Jahren haben die Angriffe auf das Online-Banking deutlich zugenommen. Manche Banken sind inzwischen nicht mehr so umgänglich, wenn es um die Reglung derartiger Schäden geht.
Die hier dargelegte Analyse und die verschiedenen Lösungsmöglichkeiten sollen Anregungen für ein sicheres Online-Banking geben.

2 Analyse

Mutmaßliches Ziel der Angreifer ist es, möglichst viel Geld von vielen Online-Konten zu ihren Finanzagenten[1] zu verfügen. Daher richten sich die Angriffe auf das größte „Potential“:

Ca. 92 % aller PC-Betriebssysteme heißen Windows, ca. 6 % Apple und weniger als 2 % Linux.
Dazu kommen die Standard Browser (InternetExplorer, Firefox, Google, Opera...).

Angegriffen wird das derzeit typische Online-Banking, bei welchem der Nutzer mit dem Browser seines Windows-PC auf die Home-Page seiner Bank geht, sich dort mit seiner PIN anmeldet und seine Verfügungen mit einer TAN autorisiert. Dabei ist es völlig unerheblich, welches TAN-Verfahren (Chip-TAN, Mobile-TAN…) angewandt wird.

Ausgeführt wird der Angriff mittels eines Trojaners, welcher meistens durch den geöffneten Anhang einer SPAM-Mail oder durch die Drive-By-Infektion einer korrumpierten Webseite auf den PC gelangt. Dort geht er in den Tarn-Modus, protokolliert das Online-Banking mit, lädt Software nach und führt beim nächsten Online-Banking des Nutzers eine verborgene, missbräuchliche Verfügung aus. Dabei sind u.a. folgende Modi bekannt:

- Der Nutzer verfügt beispielsweise 80,-€ an seinen Schornsteinfeger. Tatsächlich werden 6300,-€ an irgendein Konto in Europa überwiesen. Dem Nutzer wird seine Verfügung vorgespiegelt, welche tatsächlich aber nicht ausgeführt wurde.
- Dem Nutzer wird nach Legitimierung auf der Homepage seiner Bank ein Popup-Fenster angezeigt, wo ihm mitgeteilt wird, dass fälschlicherweise 4000,-€ von der Fa. Vodafone, Caritas, etc. auf sein Konto überwiesen wurde. Ihm wird angeboten, diese „Falschüberweisung“ durch Eingabe einer TAN zu korrigieren.
  Das Popup-Fenster kann nur durch Eingabe der TAN geschlossen werden. Dass auf seinem Konto keine 4.000,- eingegangen sind, kann der Nutzer erst in seiner nächsten Online-Banking-Sitzung erkennen.
- Dem Nutzer wird nach Legitimierung auf der Homepage seiner Bank ein Popup-Fenster mit irgendeiner Sicherheitswarnung eingeblendet. Er muss Fragen beantworten und mit einer TAN verifizieren. Anschließend kann er sein Online-Banking ausführen, ohne dass er in dieser Sitzung die missbräuchliche Verfügung, autorisiert durch die eingegebene TAN, erkennen kann.
- Dem Nutzer wird nach Legitimierung auf der Homepage seiner Bank ein Popup-Fenster mit Sicherheitswarnung eingeblendet. Er muss zur Sicherheit des Systems

1 Finanzagenten werden i.d.R. unter Vorspiegelung falscher Tatsachen über SPAM-Mails angeworben. Die Angeworbenen stellen, mitunter gutgläubig, ihre privaten Konten für Überweisungen zur Verfügung, heben eingegangene Beträge ab und leiten diese, nach Abzug einer „Bearbeitungs- oder Aufwandspauschale“ über Western Union, MoneyGram etc. weiter.

einen Transfer von 1 Cent vornehmen und mit einer TAN verifizieren. Anschließend kann er sein Online-Banking ausführen, ohne dass er in dieser Sitzung die missbräuchliche Verfügung erkennen kann.

3 Grundsätzliche Sicherheits-Aspekte

3.1 Anti-Viren-Programme

Natürlich sollte auf jedem Windows-PC ein aktuelles Anti-Viren-Programm installiert sein. Manche dieser Programme haben spezielle Sicherheitseinstellungen für das o.a. Online-Banking.
Dennoch ist festzuhalten, dass kein Anti-Viren-Programm einen 100%-igen Schutz leisten kann. Zwischen den verschieden Anbietern gibt es deutliche Unterschiede. Eine kurze Internet-Recherche (googeln) unter Verwendung der Worte „Antiviren Software Test“ führt zu aktuellen Vergleichen der gängigen Sicherheitsprogramme.

3.2 Verwendung von Kennwörtern

Zugangs-Kennwörter sind das A&O der IT-Sicherheit. Daher sollten sie so gewählt werden, dass sie weder leicht zu erraten, noch durch Brute-Force-Angriffe zu überwinden sind. Dazu gehört auch, dass die verwendeten Kennwörter keinerlei Bezug zum Nutzer haben:

- Keine Namen (Familienangehörige, Freunde, Hund, Katze, Vereine…) verwenden,
- Groß-, Kleinschreibung, Zahlen sowie Sonderzeichen einsetzen,
- ausreichend lange Kennwörter wählen und
- keinesfalls gleiche Kennwörter für verschiedene Zugänge verwenden.

3.3 Routereinstellungen

In der Regel ist heute ein Router der Einstieg ins Internet. Daher bietet es sich geradezu an, diesen anzugreifen, um in das dahinter liegende Netz eindringen zu können. Darüber hinaus bieten viele Router auch die Möglichkeit, den DNS-Server individuell, und somit auch nach Belieben eines erfolgreichen Angreifers einzustellen.

3.3.1 Kennwörter und Fernzugang

Das Standard-Kennwort eines Routers sollte nach den o.a. Kriterien geändert werden. Sofern ein Fernzugang über das Internet nicht zwingend erforderlich ist, sollte dieser abgeschaltet werden.

3.3.2 WPS

Mit WPS (Wi-Fi Protected Setup) können technisch weniger versierte Nutzer neue Geräte auf einfache Weise ins WLAN einbinden. Nun hat sich aber herausgestellt, dass genau dieses Feature ein Sicherheitsrisiko darstellt.
WPS sollte daher abgeschaltet werden.

3.3.3 WLAN

Eine gute Verschlüsselung des WLAN ist unverzichtbar. Nach heutigem Standard ist WPA2 mit einem Kennwort nach o.a. Kriterien, nicht unter 16 Zeichen zu verwenden. Je länger die Zeichenkette ist, um so sicherer ist das WLAN.

4 Lösungen

Als erste Voraussetzung sollte der Online-Verfügungsrahmen, welcher von den Banken standardmäßig zwischen 2.000,-€ und 5.000,-€ (beim Privatkunden) festgesetzt wird, auf das absolut notwendige minimiert werden. Übersteigt eine Online-Verfügung den festgesetzten Rahmen, wird diese nicht ausgeführt!
Bei seltenen höheren Verfügungen kann man seine Bank anrufen, welche den Rahmen dann kurzzeitig höher setzt.

Diese Sicherheitsmaßnahme kann aber nur im privaten, nicht im geschäftlichen Online-Banking greifen, wo ständig höhere Verfügungen getätigt werden müssen.

In der Analyse wurde dargelegt, dass sich die Gefahr eines Angriffs aus der normalen Nutzung eines PC ergibt.

Was läge näher, als das Online-Banking mit einem PC zu betreiben, welcher ausschließlich dafür - und für nichts anderes - genutzt wird.
In diesem Fall stellt sich die Frage, wie ein Trojaner dann noch implementiert werden soll.

Diese Sicherheit wird noch deutlich erhöht, wenn man ein Betriebssystem verwendet, welches eben nicht im Focus der Angreifer steht.

Hier ist aber zu beachten, dass manche Privatpersonen und erst recht manche Firmen auf die Nutzung eines Windows-PC, teilweise in einem Netzwerk mit gegenseitigem Datenaustausch bezüglich vorgenommener Transaktionen, angewiesen sind.

Unter solchen Voraussetzungen ist ernsthaft zu prüfen, einen Windows-PC ausschließlich fürs Online-Banking einzusetzen und keine weitere Internet-Aktivität zuzulassen.

4.1 Lösungen unter Windows

Eine sinnvolle Lösung ist die Nutzung eines speziellen Programms, um den Browser fürs Online-Banking auszuschließen. Darüber hinaus beherrschen die u.a. Programme das HBCI-Verfahren, welches die Sicherheit deutlich erhöht. Angriffe auf diese Programme sind mir bisher nicht bekannt, auszuschließen sind sie jedoch nicht. Die folgende Aufzählung ist nicht abschließend:

- **SFirm** wird vorwiegend von den Sparkassen angeboten,
- **ProfiCash** wird vorwiegend von den Volks- und Raiffeisenbanken angeboten,
- **VRNetworld** wird ebenfalls von den Volks- und Raiffeisenbanken angeboten und ist inzwischen meistens kostenpflichtig.
- **Hibiscus** ist kostenfrei und funktioniert auf Windows-, Apple- und Linux-Systemen,
- **StarMoney** ist ein kostenpflichtiges Programm der Fa. Star Finanz GmbH,
- **VR-Protect** nimmt einen Sonderstatus ein. Es wird in einem eigenen, gegen Windows abgeschlossenen Bereich ausgeführt. Einige Banken garantieren 100%-igen Ersatz, falls es bei Einsatz dieses Programms zu missbräuchlichen Verfügungen kommen sollte.

  Zitat: Über den Banking-Browser VR-Protect öffnen Sie Ihr Online-Banking in einem Bereich, in den man von außen nicht eindringen kann. So bewegen Sie sich in einer Schutzzone außerhalb des Zugriffsbereichs von Datendieben.

4.2 Wirklich sicheres Online-Banking

Wie schon erwähnt ist ein separates Betriebssystem, welches nicht im Focus der Angriffe steht, fürs ausschließliche Online Banking vorzuziehen. Dafür bietet sich das kostenfreie Linux geradezu an.

Die Lösung heißt also: Ein Linux-PC ausschließlich fürs Online-Banking.

Nun hat nicht jeder mal einen oder mehrere PC übrig, welche er entsprechend einsetzen kann. Das ist auch nicht nötig, hier gibt es folgende Alternativen:

4.2.1 Online-Banking-DVD

Eigentlich braucht man nur eine Live-CD fürs Online-Banking. Hier bieten sich mehrere an: Knoppix, Ubuntu, Lubuntu…

Zielgerichtet sind aber so genannte Online-Banking-DVD, welche dafür besonders angepasst und abgesichert sind:

- c`t Bankix
- PC-Welt Banking DVD
- com!-Fox
- …

Positiv getestet wurde hier die c`t Bankix. Leider wird dieses „Programm“ inzwischen nicht mehr gepflegt. Wesentlich ist aber, dass solche Tools gepflegt werden, sodass man auch neuere Versionen erhalten kann.

Nachteil dieser sehr sicheren Lösung ist die Boot-Dauer einer CD/DVD und die Erforderlichkeit eines LAN-Anschlusses. Bei einem Notebook mit WLAN-Anschluss wird’s kompliziert.
Darüber hinaus muss das Bios so angepasst werden, dass von der CD gebootet werden kann.

4.2.2 Online-Banking-Stick

Die o.a. CD/DVD können z.B. mit der kostenfreien Software Unetbootin auf einen USB-Stick gebracht werden. Damit bootet es sich deutlich schneller und zumindest bei der c`t Bankix kann bei erstmaligem Gebrauch ein WLAN-Anschluss dauerhaft konfiguriert werden.
Darüber hinaus muss das Bios so angepasst werden, dass vom USB-Stick gebootet werden kann.

4.2.3 Zusätzliche Linux-Boot-Partition

Linux kann aber auch zusätzlich zu einem Windows-Betriebssystem auf der Festplatte des PC installiert werden. Beim Systemstart erscheint dann ein Auswahlmenü mit den Betriebssystemen Windows und Linux.
Linux auswählen fürs Online-Banking, Windows für alles andere.

4.2.4 Linux in einer virtuellen Maschine unter Windows

Nun gibt es einige wenige Hardware-Konfigurationen, auf welchen Linux ohne individuelle Anpassung nicht startet. Eine solche Anpassung erfordert differenzierte Linux-Kenntnisse.

Hier kann man Linux auch in einer so genannten virtuellen Maschine unter Windows installieren. Dann läuft Linux einfach als unabhängiges Betriebssystem in einem Windows-Fenster. Da sich die virtuelle Maschine der Schnittstellen von Windows

bedient, gibt es keine Hardware-Probleme.
Natürlich sollte man zwischen der virtuellen Maschine und dem Windows Host keine Zugriffe z.B. über gemeinsame Ordner erlauben, das ist aber bereits die Standard-Einrichtung.

Zum Einrichten eines virtuellen PC gibt es beispielsweise die Virtualbox oder den VMWare-Player, welche beide für den Privatgebrauch kostenlos sind.

5 Nachbemerkung

Die dargelegten Lösungen stellen den Stand von heute dar.
Darüber hinaus ersetzen sie nicht den sorgfältigen und kritischen Umgang des Anwenders mit seinem PC und dem Internet.

Die nachfolgend aufgeführten Quellen und Hinweise erweitern und vertiefen das Thema.

Quellen und weitere Hinweise:

http://de.norton.com/dos-donts-passwords/article

http://www.zdnet.de/41559071/update-30-12-us-cert-warnt-wlan-router-unsicher-durch-wps/?PageSpeed=noscript

https://www.voba-si.de/wir-fuer-sie/presse/2014-08-25OnlineGarantie.html

http://www.banktip.de/rubrik2/20223/sicheres-online-banking-die-bank-auf-cd.html

http://www.pcwelt.de/ratgeber/Die_PC-WELT_Online-Banking-DVD-Sicherheit-8815632.html

http://www.heise.de/ct/projekte/Sicheres-Online-Banking-mit-Bankix-284099.html

http://www.com-magazin.de/news/sicherheit/7-tools-sicheres-online-banking-65442.html

http://www.com-magazin.de/praxis/internet/sicheres-homebanking-mit-com-fox-38299.html

http://www.heise.de/download/virtualbox.html

http://www.heise.de/download/vmware-player.html