



G Data

Whitepaper 12/2009

Sicheres Onlineshopping: Weihnachtsgeschenke aus dem Web richtig einkaufen.

Sabrina Berkenkopf & Ralf Benzmüller
G Data Security Labs

Geschützt. Geschützter. G Data.



Inhalt

Onlineshopping seit Jahren im Aufwind	2
Phishing: Angriff auf Käuferdaten	2
Sicherheitsmerkmale von Webseiten und Onlineshops	4
Der richtige Umgang mit Passwörtern	5
Eine gesicherte Umgebung ist wichtig!.....	6
Kurz zusammengefasst	7

Onlineshopping seit Jahren im Aufwind

Die Beliebtheit des Onlinehandels ist in den letzten Jahren innerhalb der EU stetig gewachsen. 2008 benutzten fast ein Drittel (32%) der Europäer im Alter zwischen 16 und 74 Jahren das Internet, um Waren und Dienstleistungen für den persönlichen Gebrauch zu bestellen. Diese Zahl beschreibt einen Anstieg um 12% innerhalb von vier Jahren. In Deutschland gaben mehr als die Hälfte der befragten Personen (53%) an, online einzukaufen, in Frankreich 40%, in Spanien 20% und in Polen 18% (Quelle: Eurostat). Die Weihnachtsmonate November und Dezember bescherten dem Onlinehandel mit Waren 2008 rund 2,7 Mrd. Euro Umsatz, was einem Plus von 23% entspricht, so der Bundesverband des Deutschen Versandhandels e.V. (Quelle: bvh e.V.).

Der Branchenverband Bitkom sieht für das Jahr 2009 14,3 Millionen weihnachtliche Onlineshopper, was gegenüber 2008 ein Drittel Zuwachs bedeutet. Zusätzliche 8,6 Millionen Nutzer seien noch unentschlossen (Quelle: Bitkom). Die Prognosen der Experten weisen zudem weiter steigende Nutzer- und Umsatzzahlen für die Zukunft des Onlinehandels aus.

Phishing: Angriff auf Käuferdaten

Der Diebstahl und Missbrauch persönlicher Daten hat in den vergangenen Jahren deutlich zugenommen. Besonders lukrativ ist für Onlinekriminelle der Verkauf von Kreditkarten-Informationen, Onlinebanking-Accounts und Zugangsdaten zu Treuhandservices, wie PayPal. Phishing beschreibt das Ausspionieren und Abgreifen von persönlichen Daten jeglicher Art von einem Computer. Die Ziele der Cyberkriminellen sind dabei vor allem Passwörter und Zugangsdaten zu Benutzerkonten von zum Beispiel Onlinebanking, Bezahldiensten, Handelsplattformen, sozialen Netzwerken und Onlinespielen. Bitkom veröffentlichte in Zusammenarbeit mit dem BKA die Information, dass 5% der Internet-Nutzer ab 14 Jahren Opfer von Phishing wurden. Bitkom prognostiziert Deutschland für das Jahr 2009 einen Schaden von 10,9 Mio. Euro durch illegale Geldströme nach Phishing, was einen Zuwachs von 56% gegenüber 2008 bedeuten würde.



Abb. 1: Screenshot einer PayPal Phishing-Mail

Die häufigste Masche, um an die Daten der Nutzer zu kommen, ist der Versand von Phishing E-Mails, die in ihrem Design sehr häufig an das großer, seriöser Unternehmen angepasst sind oder dieses sogar komplett kopieren. Waren Phishing E-Mails früher häufig sofort durch eklatante Rechtschreibleistungen, Grammatikfehler, fehlende Umlaute und Sonderzeichen zu entlarven, sind sie heute in Form und Sprache oft tadellos und somit nicht mehr auf den ersten Blick zu erkennen. Renommiertere Banken, Versanddienstleister mit Packstationen und Computerspielhersteller sind sehr beliebte Vorlagen für diese E-Mails.

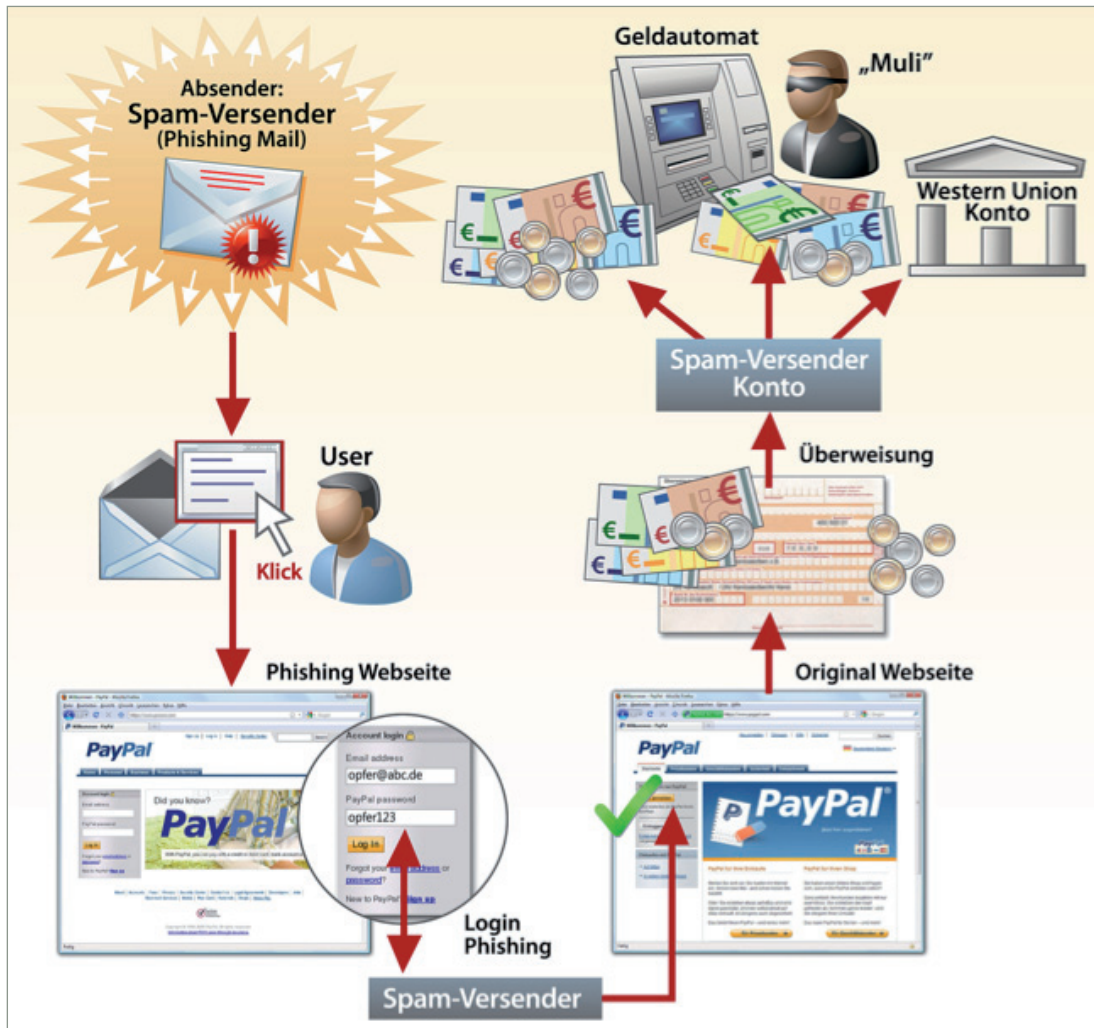


Abb. 2: Schaubild eines Phishing-Angriffs

Der Empfänger einer Phishing E-Mail wird aufgefordert, einem Link zu folgen und seine Zugangsdaten auf dieser Webseite einzugeben. Beliebte Masche ist dabei die Masche, dass dem Empfänger vorgegaukelt wird, die in der E-Mail erwähnte Webseite seines Vertrauens (z.B. eBay, PayPal oder andere) hätte die Sicherheitsrichtlinien aktualisiert und dafür müsste sich der Benutzer nun anmelden, um diese zu akzeptieren/sich dafür zu registrieren. In anderen Fällen wird der E-Mail Empfänger gebeten, seine persönlichen Daten zu aktualisieren und wird mit dem eingebetteten Link auf eine Betrugsseite gelotst. Eine weitere Masche, die gerade zur Weihnachtszeit durch die hohe Anzahl an Paketsendungen kritisch ist, lässt den Nutzer glauben, dass er sich auf einer Seite anmelden muss, um seinen persönlichen Postversandstatus der bestellten (Weihnachts-)Einkäufe anzusehen.

Dabei sind die verlinkten, betrügerischen Webseiten häufig kaum vom Original zu unterscheiden. Wer hier nun nach der Aufforderung Benutzernamen, Passwörter, Kontonummern, PINs, TANs oder ähnliches preisgibt, kann ausspioniert und (finanziell) geschädigt werden.

Gelingt es den Bösewichten zusätzlich, die Zugangsdaten zum E-Mail Account des Betroffenen zu erlangen, können sie sich sogar über die oft vorhandene Funktion „Passwort neu zusenden“ neue Passwörter für die verschiedenen Kanäle zuschicken lassen. Und mit dem entführten E-Mail Konto lassen sich dann auch weitere, neue Shopping-Accounts anlegen und der Schaden kann steigen.

Bei der beschriebenen Art von Phishing ist der Benutzer das schwächste Glied in der Kette der Sicherheitsmaßnahmen. Nur wenn der Nutzer seine Daten „freiwillig“ eingibt, gelangen sie in Hände von Cyberkriminellen. Daher gilt: E-Mails von unbekanntem Absendern sollten misstrauisch behandelt werden. Es sollten keine Links angeklickt werden, die auf Anmeldeseiten, z.B. von angeblichen Bankenportalen, eBay, Postämtern oder ähnlichen führen sollen. Seriöse Unternehmen fragen keine Kundendaten oder Zugangsdaten per E-Mail ab!

Sicherheitsmerkmale von Webseiten und Onlineshops

Der Empfänger sollte sich nach dem Erhalt der E-Mail nicht bedroht oder genötigt fühlen, sofort (!) die verlinkte Seite aufzurufen, da ihm in der E-Mail diese und jene Konsequenzen angedroht werden, wenn er dies nicht tut. Der Link aus der E-Mail sollte einfach ignoriert werden.

Webadressen sollten am besten immer manuell in die Adresszeile des Browsers eingegeben oder über die persönlichen Lesezeichen aufgerufen werden. Hat ein Kunde nun eine Seite besucht, die besonders sensibel mit den persönlichen Daten umgehen muss, sollte zusätzlich auf folgende möglichen Sicherheitsmerkmale geachtet werden: ein angezeigtes Vorhängeschloss-Symbol im Browser und den Zusatz „https“ am Anfang der Webadresse. Neuerdings wird in vielen Webbrowsern eine verschlüsselte Webseite auch durch eine grün eingefärbte Adresszeile angezeigt.



Abb. 3: Screenshot einer sicheren Seite im Mozilla Firefox 3.5

Diese Sicherheitsmerkmale sind nicht nur auf Bankseiten zu beachten, sondern sichern auch direkte Bezahlungen in Onlineshops beim Kauf per Kreditkarte oder Lastschriftverfahren und das Einloggen auf seriösen Bezahlendiensten (wie z.B. PayPal). Erfordert ein Onlineshop eine vorherige Registrierung des Käufers, sollten auch diese persönlichen Registrierungsdaten über eine soeben beschriebene, gesicherte, Verbindung an den Händler geschickt werden können. Der aktuelle Internet Explorer 8 zeigt außerdem die Top Level Domain der aktuellen Webseite in schwarzen Buchstaben an und die restlichen Adressteile in grau. So kann sichergestellt werden, dass man auch wirklich auf einer offiziellen Seite von z.B. eBay landet und nicht auf einer falschen Adresse, die nur eBay zur Täuschung als Namensbestandteil hat.



Abb. 4: Screenshot einer sicheren Seite im Internet Explorer 8

Außerdem sollte darauf geachtet werden, dass die ausgesuchten Onlineshops vertrauenswürdig sind. Große und weltweit bekannte Anbieter (wie z.B. amazon.com) haben eine positive Reputation und sind im Onlinehandel etabliert. Wenn man sich jedoch einen weniger bekannten Anbieter ausgesucht hat, können folgende Fakten Aufschluss über die Authentizität geben:

- Ist der angebotene Preis für ein Produkt „im Rahmen“, oder ist er unnatürlich niedrig?
- Stimmen die Produktbeschreibungen und -fotos?
- Sind die Versandkosten klar ersichtlich und angemessen?
- Hat der Onlineshop gut ausgewiesene Allgemeine Geschäftsbedingungen (AGBs)?
- Stimme ich den in den AGBs aufgeführten Angaben und Bedingungen zu?
- Hat die Webseite ein Impressum?
- Kann ich den Shop in Suchmaschinen finden? Ist er bekannt?

Der richtige Umgang mit Passwörtern

Zur Anmeldung sollten starke Passwörter ausgewählt werden. Passwörter wie „admin“ oder „passwort123“ gehören nicht in diese Kategorie! Eine Kombination aus mindestens 8 Buchstaben in Groß- und Kleinschreibung, Ziffern und Sonderzeichen generiert starke Passwörter, wie z.B. „Hb1&opGT58“. Diese genannte Zeichenfolge ist ein fiktiv zusammengestelltes Passwort, das sicher ist, aber man kann es sich nur schwer merken. Um sich ein Passwort mit persönlichem Wiedererkennungswert zu erstellen, können unter anderem Akronyme verwendet werden:

The sound of silence von Simon & Garfunkel von 1966 = TsovsS&Gv1966

Auch die Benutzung von so genannter „Leetspeak“ ist möglich, wobei Buchstaben durch ähnlich aussehende Ziffern und Sonderzeichen ersetzt werden:

The sound of silence = 7h3_50und_of_51l3nc3

Generell sollten Benutzernamen und Passwörter nicht im Browser gespeichert werden, auch wenn das sehr bequem erscheint. Durch gespeicherte Log-in Daten und andere persönliche Informationen macht man sich angreifbar für eine weitere Art des Phishings: Angriff durch Trojanische Pferde.

Trojanische Pferde schleusen ein Schadprogramm auf den Computer des Benutzers und führen dort unerwünschte Vorgänge aus. Einer der möglichen Vorgänge spioniert mit sogenannter Spyware persönliche Daten auf dem befallenen Computer aus und übermittelt diese dann an eine vorher durch den Programmierer des Trojanischen Pferdes festgelegte Adresse im Internet. So gelangen Cyberkriminelle dann auch ohne die aktive Hilfe des Benutzers an dessen Daten.

Eine gesicherte Umgebung ist wichtig!

Onlineshopping, Onlinebanking und andere sensible Vorgänge sollten nicht über ein öffentliches WLAN oder aus einem Internetcafé ausgeführt werden. Die Gefahr des Datenraubs, durch z.B. Sniffer, ist bei frei benutzbaren, ungesicherten WLAN Access Points unkalkulierbar hoch. In Internetcafés könnten Cookies und andere auf den Benutzer bezogene Logs mit persönlichen Daten nach dem Surfen auf dem öffentlichen Rechner verbleiben und für nachfolgende Benutzer einsehbar und verwendbar sein. Im Regelfall haben Besucher eines Internetcafés auch keine Kontrolle über die Sicherheitseinstellungen des Computers und müssen sich somit auf das Know-how und Sicherheitsbewusstsein des Cafébetreibers einlassen und verlassen.

Die soeben aufgezählten Gefahren und ihre Wirksamkeit sind abhängig vom gesunden Menschenverstand des Benutzers. Jedoch sollte man auf keinen Fall vergessen, dass der Computer ebenfalls eine Hauptrolle beim Onlineshopping spielt:

Ein Computer sollte mit einer zuverlässigen Antivirenlösung, Firewall und auch einem HTTP-Filter ausgerüstet sein. So kann sich der Benutzer in Echtzeit mit der Antivirensoftware vor vielerlei Schädlingen (Trojanischen Pferden, Viren, Würmern, etc.) schützen, seine E-Mails auf Phishing, Spam (wie z.B. Casino Einladungen und diverse Pharmaerzeugnisse) und Schädlinge scannen und auf diese und andere ungewünschte Inhalte filtern lassen. Zusätzlich kann ein HTTP-Filter den gesamten eingehenden und ausgehenden Onlineverkehr live scannen und Bedrohungen direkt blocken, damit schädliche Webseiten dem Benutzer keine ungewollten Inhalte, wie z.B. das aktuell wieder grassierende Trojanische Pferd „Gumblar“, unterschieben können. Eine Firewall regelt den kompletten Datenverkehr nach vordefinierten Regeln und unterbindet ihn gegebenenfalls, damit Angreifer keine offenen Türen in den Computer nutzen können.

Angreifer setzen verstärkt auf Sicherheitslücken in den Systemen Ihrer Opfer, die auf ein vernachlässigtes Update-Management zurückzuführen sind, daher muss die Antivirenlösung und ihre Komponenten immer auf dem aktuellsten Stand gehalten werden. Meistens verfügen die Programme über eigene Update-Routinen, die diese Aufgabe automatisch erledigen. Es empfiehlt sich, vor dem Beginn der Onlineshopping-Tour alle Komponenten zu aktualisieren und einen Komplettsan des Rechners durchzuführen, damit der Computer nicht durch eventuell schon im System vorhandene Schädlinge angreifbar ist.

Aber nicht nur das Schutzprogramm sollte up to date sein, sondern auch das Betriebssystem durch Updates immer auf den neuesten Stand gebracht werden. Auch diese Funktion ist in den meisten Betriebssystemen automatisch anwendbar. Zusätzlich dazu sollte auch der Browser regelmäßig aktualisiert werden, denn er ist naturgemäß besonders anfällig für Angriffe aus dem Internet und bietet Sicherheitslücken, wenn seine Version veraltet ist. Gleiches gilt für die E-Mail Programme, Chat-Programm, FTP-Programme, Grafik- und Videosoftware sowie die restliche auf dem Computer installierte Software.

Kurz zusammengefasst:

Die G Data Software AG empfiehlt folgende sechs Maßnahmen, um ein mögliches Risiko beim weihnachtlichen Onlineshopping zu minimieren:

1. Benutzen Sie eine aktuelle Antivirenlösung, eine Firewall und einen HTTP-Filter
2. Halten Sie die Sicherheitssoftware, das Betriebssystem und andere Software auf dem aktuellsten Stand.
3. Seien Sie misstrauisch bei E-Mails von fremden Absendern – Klicken Sie keine Links an und laden oder öffnen Sie keine angehängten Dateien
4. Geben Sie Adressen von Webseiten mit Benutzeranmeldung manuell ein oder benutzen Sie die Lesezeichenfunktion Ihres Browsers
5. Achten Sie auf die Sicherheitsmerkmale im Browserfenster, wenn Sie online einkaufen:
 - Das Vorhängeschloss im Browser
 - Die Abkürzung „https“ vor der eingegebenen Adresse
 - Die grün hinterlegte Adresszeile in vielen modernen Browsern
 - Die Anzeige der richtigen Top-Level Domain, speziell im Internet Explorer 8
6. Kontrollieren Sie, ob der Shop Ihrer Wahl über AGBs, Impressum und übersichtliche Kostenaufstellungen verfügt (z.B. Versandkosten und evtl. Zusatzkosten)