KANTON LUZERN

Datenschutzbeauftragter
des Kantons Luzern
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 66 06
dsb@lu.ch
www.datenschutz.lu.ch

Merkblatt "Phishing"[1]

1. Zweck des Merkblattes

Das Phishing ist eine spezielle Form des Social Engineerings. Unter Social Engineering versteht man das Ausnützen von Hilfsbereitschaft, Gutgläubigkeit und Unsicherheit, um an vertrauliche Daten zu gelangen. Das Social Engineering gilt als eine der erfolgreichsten Angriffsmöglichkeiten der heutigen Zeit.

Phishing, ein Kunstwort gebildet aus "password fishing", ist derzeit in aller Munde. Man versteht darunter die Methode, mit der Phisher versuchen, mit Hilfe von gefälschten E-Mails an vertrauliche Kundendaten zu gelangen.

Anwender erhalten ein professionell aufbereitetes E-Mail, das vermeintlich von ihrer Bank, einem Kreditkartenunternehmen, einem Online-Bezahlinstitut wie Paypal oder auch von E-Bay stammt[2], in dem sie zum Aktualisieren ihrer Benutzerdaten aufgefordert werden. Die Mails enthalten Links zu gefälschten Webseiten, die der originalen Website des vermeintlichen Absenders zum Verwechseln ähnlich sehen. Dort werden die Kunden angehalten, persönliche Daten wie Vertragsnummer, Passwörter oder Kreditkarten-Nummern einzugeben, welche im Hintergrund abgefangen und missbraucht werden.

Auf die Phishing-Attacken fallen keineswegs nur vertrauensselige Zeitgenossen herein, auch Internetprofis zählen zu den Opfern. Gefährdet sind nicht nur Nutzer des Online-Banking, sondern auch Kunden von Internet-Auktionshäusern, bei welchen es darum geht, an die Kreditkarten-Informationen zu gelangen.

Dieses Merkblatt soll aufzeigen, wo die Gefahren des Phishings liegen und wie sich ein Internet-Benutzer optimal gegen Phishing-Attacken schützen kann.

2. So funktioniert das Phishing[3]

- Die Betrüger kopieren das Layout der Website einer Bank oder eines ähnlichen Instituts und programmieren sie so, dass sie ihnen die eingegebenen Daten übermittelt. Die Site wird irgendwo im Internet gespeichert, unter Umständen auf einem gehackten Server, dessen Betreiber davon nichts weiß[4]. Der Domain-Name wird so gewählt, dass er wie

[1] Phishing wird im Englischen oft auch Scam- oder Fraudster-Angriff genannt.
[2] Die E-Mail-Absender-Adresse ist bei Phishing-Mails gefälscht.
[3] Auf der Site der Cybernetguard kann ein PHISHING-Demonstration angeschaut werden: http://www.cybernetguard.ch/phishing/
[4] Dadurch ist es oft schwer, die Phisher ausfindig zu machen.

ein echter Name des Geldinstituts aussieht. Eine andere Möglichkeit für Phishing besteht darin, dass mit einem Script die Adresszeile im Browser mit einem Bild überdeckt, das die Adresse der vertrauenswürdigen Site vorgaukelt.

Ein Beispiel für die Überlagerung der Adresszeile mit einer falschen Adresse sehen Sie hier:

Ein Script (1) kann die Adresszeile Ihres Browsers mit einer Grafik, in diesem Beispiel ein Bild mit einer Adressezeile darin, überdecken.

Damit wird Ihnen die korrekte Adresse (2) angezeigt, obwohl Sie sich auf einer anderen Website befinden.

1)

2)

- Mit Massenmails werden die Kunden des Geldinstituts zur Aktualisierung ihrer persönlichen Daten aufgefordert. Die Mails werden sprachlich und vom Erscheinungsbild her ebenfalls im offiziellen Stil des vermeintlichen Absenders gehalten. Ein Link im E-Mail führt zur gefälschten Website. Dabei werden die verunsicherten Empfänger oft psychologisch unter Druck gesetzt. Das Schreiben warnt sie beispielsweise, dass ihr Konto gehackt wurde und neu verifiziert werden muss. Falls die Daten nicht sofort aktualisiert werden, werde das Konto gesperrt.

- Unvorsichtige Internet-Nutzer kommen der Aufforderung nach, klicken auf den angegebenen Link und tragen ihre Benutzerdaten auf der gefälschten Website ein.

- Von der gefälschten Website werden die Eingaben zu einem Postfach gesendet, das die Betrüger bei einem Gratismailservice angelegt haben. Mit den erbeuteten Codes verschaffen sich die Betrüger Zugang zu Konten auf der originalen Site und tätigen dort Überweisungen oder missbrauchen die Kreditkarteninformationen für Transaktionen und Einkäufe.

- Gute Phisher zeigen den Anwender nach dem Abfangen der Daten eine Fehlerseite an, dass die Informationen nicht übermittelt werden konnten und springen direkt auf die originale Website weiter. Dadurch erfährt der Anwender nicht, dass seine Benutzerdaten geklaut wurden und den Phishern bleibt genug Zeit die Zugangsdaten oder Kreditkarten-Informationen zu missbrauchen.

Während in der Anfangsphase des Phishings bereits an der schlechten Formulierung oder an den fehlerhaft übersetzten englischen Texten erkennbar war, dass ein E-Mail nicht echt ist, so kommen die Mails heute professioneller daher. Auch die Qualität der gefälschten Internet-Auftritte wird besser und besser. Die Seiten werden heute so täuschend echt nachgebaut, dass sogar das Zeichen für eine verschlüsselte SSL-Verbindung in der Statusleiste des Browsers auftaucht, obwohl keine SSL-Verbindung verwendet wird. Mit einem Doppelklick auf das Schlüsselsymbol kann aber immer noch geprüft werden, ob eine SSL-Verbindung verwendet wird und ob man sich tatsächlich auf der gewünschten Seite befindet.

Es sind auch Fälle bekannt, bei welchen die Phisher im Hintergrund die echte Website anzeigen lassen, aber mit einem Pop-up-Fenster überlagern, um an die persönlichen Daten zu gelangen.

3. So schützen Sie sich vor Phishing

Folgende Grundregeln sollten Sie unbedingt einhalten, um Phishing abzuwenden:

- Nehmen Sie die Absender von Mails und die Betreiber von Websites genau unter die Lupe und hinterfragen Sie den Inhalt kritisch. Denken Sie daran, dass der Domain-Namen (www.meineBank.ch) keine Aussage über den Betreiber macht. Es kann sich gut um eine Fälschung handeln. Behalten Sie auch immer im Hinterkopf, dass eine seriöse Bank Sie niemals per Mail auffordern würde, dass Sie ihre Benutzerdaten neu erfassen.

- Den Website-Namen Ihrer Bank, Ihres Kreditkartenunternehmens etc. sollten Sie ausschließlich selber eingeben (oder zumindest über eigene Bookmarks öffnen) und nicht über Links aufrufen, weil anhand des angezeigten Linknamens nicht ersichtlich ist, welche Seite aufgerufen wird.

- Wenn Sie über einen Link in einem E-Mail zu einer Site gelangen, die ein Login mit Kontodaten, Kreditkartennummern und Passwörtern verlangt, brechen Sie die Aktion ab.

- Schützen Sie Ihren Rechner mit einem aktuellen Virenscanner und einer Firewall. Achten Sie zudem darauf, dass Sie immer die aktuelle Systemsoftware und die aktuelle Browserversion mit allen Sicherheitspatches verwenden.

Sollte Ihre Anti-Viren-Software ein Phishing-Mail erkennen oder sollten Sie ein E-Mail erhalten, bei welchem Sie glauben, dass es sich um Phishing handelt, so versuchen Sie im Internet herauszufinden, ob diese Attacke bereits bekannt ist. Wenn nicht, so informieren Sie das betreffende Unternehmen und senden Sie das Mail cc: an die Anti-Phishing Working Group (reportphishing@antiphishing.org). Sie können auf diese Weise dazu beitragen, dass viele andere gefährdete Anwender vor einem Betrug bewahrt werden.

4. Technische Hilfsmittel gegen Phishing für Anwender

Im Wettlauf mit den Phishing-Attacken haben einige Unternehmen Tools entwickelt, die den Anwender vor Phishing schützen sollen. Es folgt eine nicht abschliessende Liste von kostenlosen derartigen Programmen:

- Spoofstick von CoreStreet zeigt den tatsächlichen Servernamen auf einer Website an.

- Cloudmark Antifraud Toolbar, GeoTrust TrustWatch, Earthlink Toolbar beurteilen Websiten über ein White-/Blacklist-System. In den meisten Fällen sind die geführten Listen von betrügerischen Websites allerdings nicht genügend aktuell, um tatsächlich Sicherheit zu gewährleisten.

- eBay Toolbar von eBay und PwdHash von der Universität Stanford bieten Schutz vor Passwortmissbrauch durch gefälschte Seiten und Schutz der Browserleisten vor Manipulationen.

- Netcraft Toolbar, Fraud Eliminator von Infini, Comodo TrustToolbar und Spoofguard von der Stanford Universität vereinigen mehrere Methoden wie beispielsweise Black-/Whitelisten, URL-Checking, Echtzeit-Seitenanalyse, Domain-Checking, Passwort-Schutz und Schutz der Browserleisten.

Auch die gängigen AntiViren-Hersteller haben auf die Phishing-Problematik reagiert. Wo vor einigen Monaten noch keine Warnung ausgegeben wurde, erkennen die neusten Updates heute Phishing-Attacken und warnen die Anwender oder lassen einen Zugriff auf diese Websites gar nicht mehr zu.
Wie in anderen Bereichen gilt auch hier, dass die Programme keinen vollständigen Schutz bieten können. Entscheidend bei der Abwehr von Phishing ist nach wie vor die Aufmerksamkeit der Anwender.

5. Fragen und Informationen

Für Fragen und weitere Informationen zum Thema Phishing stehen Ihnen die Datenschutzbeauftragten gerne zur Verfügung.

Postadresse:	Datenschutzbeauftragte des Kantons Luzern Bahnhofstrasse 15 6002 Luzern
Telefon:	+ 41 41 228 66 06
Fax:	+ 41 41 228 69 13
Internet:	http://www.datenschutz.lu.ch
E-Mail:	dsb@lu.ch **WARNUNG**: Der E-Mail-Verkehr ist unsicher. Vertrauliches gehört deshalb nicht in E-Mails!

Luzern, Februar 2005 (Aktualisiert Oktober 2005)