E-Mails mit erpresserischem Inhalt im Umlauf

Art der Bedrohung

Erpressung mit angeblichen Videoaufnahmen bei sexuellen Selbsthandlungen durch vorgegebene Sicherheitslücke am Computersystem. Zur Untermauerung des Vorhaltes werden tatsächlich existente Passwörter zu den E-Mail-Konten angeführt.

Modus Operandi

In einer früheren Erscheinungsform wurden diese „Erpresser E-Mails“ wahllos an zahlreiche E-Mail Empfänger/innen versendet, wobei „auf gut Glück“ versucht wurde, eine Antwort und/oder eine Bezahlung von den vermeintlich „erwischten“ Opfern erpressen zu können.

Das angebliche Videomaterial gibt es in den seltensten Fällen, jedoch sollte man nicht außer Acht lassen, dass durch verschiedene Sicherheitslücken (sog. Exploits) in Einzelfällen auch ein widerrechtlicher Zugriff auf den Computer oder die Kamera „von außen“ möglich wäre.

Regelmäßige Updates von Hardware und Software sind daher besonders wichtig!

Aufgrund zahlreicher aktueller Anlassfälle konnte beobachtet werden, dass in den nunmehrigen Erpresser-E-Mails auch ein Passwort zum jeweiligen Mail-Account angeführt ist. Dadurch soll bei dem/der Mailempfänger/in der Glauben erwecke werden, dass das Passwort durch den Absender ausgespäht worden ist. Nach Auskunft der Opfer handelt es sich dabei durchgängig um ältere oder sehr alte Passwörter, welche aber tatsächlich in Verwendung waren und zum Teil auch noch für andere Zugänge / Dienste im Internet genutzt werden.

Bei den Daten der angeschriebenen und erpressten E-Mail-Empfänger dürfte es sich um Datensätze aus so genannten Daten-Leaks1 handeln, der genaue Ursprung ist meistens nicht zurück verfolgbar.

In diesem Zusammenhang darf auf die Tragweite bei der Preisgabe von Zugangsdaten hingewiesen werden, dass bei der Anmeldung im Internet äußerste Vorsicht geboten ist, mit welchen Zugangsdaten eine solche Anmeldung durchführt wird und wem man seine Daten anvertraut.

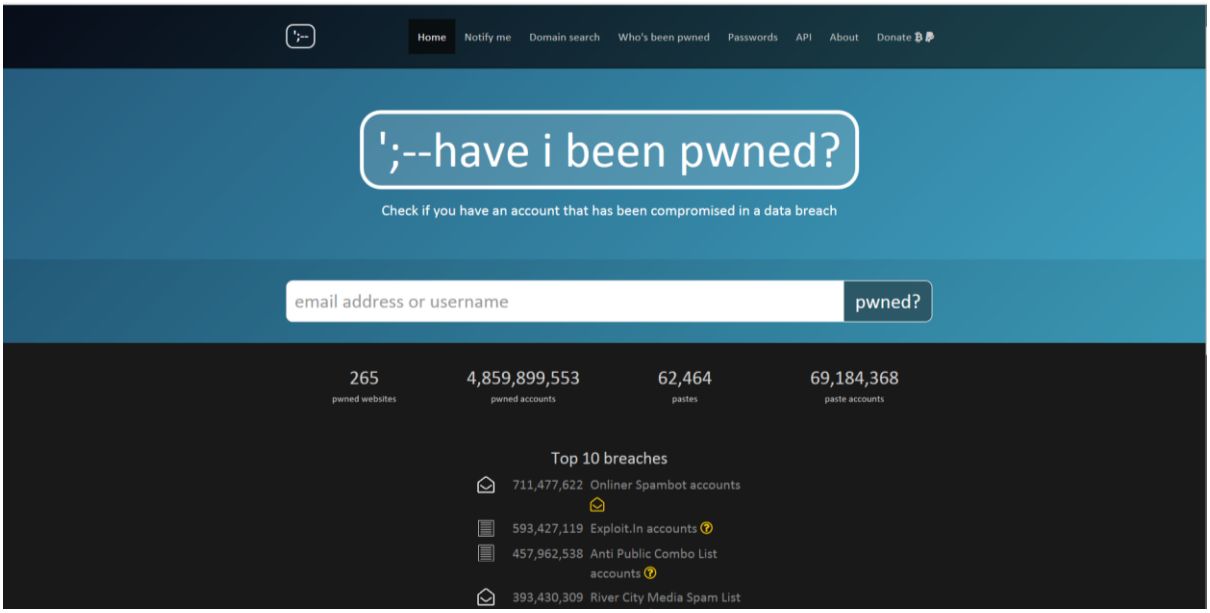
[1] https://de.wikipedia.org/wiki/Datenpanne; https://de.wikipedia.org/wiki/Leak

Empfohlene Vorgangsweise beim Erhalt einer solchen Erpresser E-Mail:

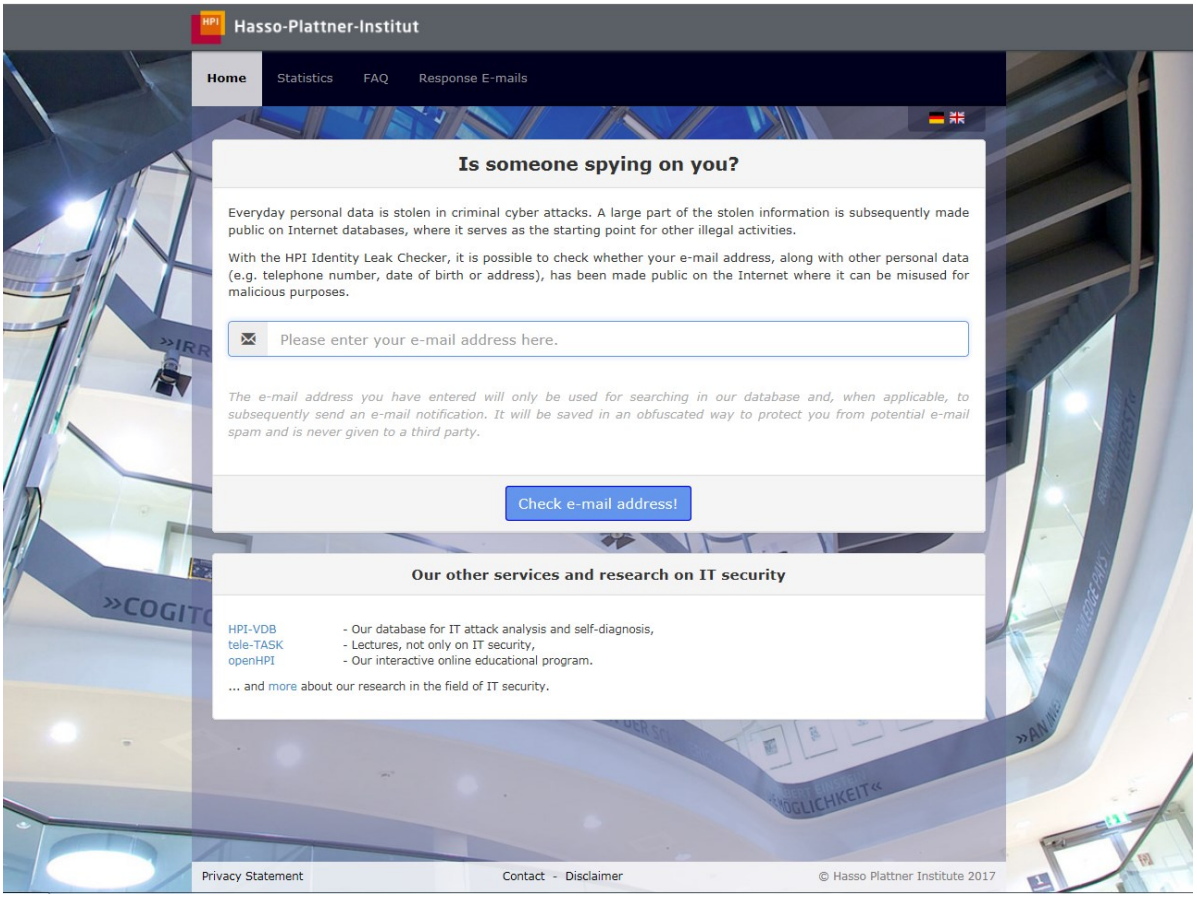
- Steigen Sie auf Geldforderungen keinesfalls ein und antworten Sie nicht auf die Erpressermail.
- Öffnen sie keine Dateianlagen oder Links bei verdächtigen Emails, weil diese Schadsoftware beinhalten könnten.
- Verschieben Sie verdächtige Emails in den Spam oder Junk-Mail Ordner oder löschen sie diese endgültig mit den Tasten Shift + Entfernen.
- Sollten Sie Webcams und Mikrofone verwenden, so sollten diese und deren Verwendung auch mittels Passwort geschützt sein. Bei (zeitweiser) Nichtverwendung sollten das Mikrofon und Objektiv abgedeckt oder abgeklebt werden, es gibt diesbezüglich wiederverwendbare Lösungen.
- Ändern Sie regelmäßig Ihre Zugangsdaten, verwenden Sie unterschiedliche und komplexe Passwörter für verschiedene Accounts und Anwendungen.
- Überprüfen Sie in regelmäßigen Abständen, ob Ihre Mail-Adresse(n) und Passwörter unter Umständen kompromittiert sind. Dies können Sie unter anderem auf der Webseite www.botfrei.de, einem kostenlosen Service des eco – Verband der Internetwirtschaft Deutschland, unter der Rubrik Werkzeuge mit den Tools „';--have i been pwned?“ und „HPI Identity Leak Checker“ durchführen.

Möglichkeiten um festzustellen, ob meine E-Mail-Adresse kompromittiert ist:

https://haveibeenpwned.com/



https://sec.hpi.uni-potsdam.de/ilc/search?lang=de/



Beachten Sie die Sicherheitshinweise und Tipps für einen Sicheren Umgang mit dem Internet und Schutz vor IT-Kriminalität der Kriminalprävention: http://www.bundeskriminalamt.at/praevention. oder http://www.bundeskriminalamt.at/202/Betrug_verhindern/start.aspx

Weiterführender Link:

Watchlist-Internet: https://www.watchlist-internet.at/news/erpressung-mit-masturbations-video/.

HERAUSGEBER: Bundesministerium für Inneres
Bundeskriminalamt
A-1090 Wien, Josef Holaubek Platz 1
Tel.: +43 1 24836 986500

FEEDBACK

NEWSLETTER AN-/ABMELDUNG