Pressefrei ab 31. Januar 2019, 11 Uhr

Safer Internet Day: Sensible Daten im Netz schützen

BSI und Polizei raten zu sicherem Umgang mit persönlichen Daten

Stuttgart/Bonn: Wenn viele persönliche Daten einer Person im Internet kursieren, kann das Folgen haben: Betrüger können damit unter falschem Namen Online-Bestellungen tätigen oder Verträge und Abonnements abschließen. Immer wieder kommt es auch zu Erpressungsfällen oder dem Bloßstellen Betroffener. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) rufen daher anlässlich des Safer Internet Day am 5. Februar 2019 zu einem umsichtigen Umgang mit persönlichen Daten im Internet auf.

„Identitätsdiebstahl ist längst zu einem Alltagsphänomen geworden, vor dem die Anwenderinnen und Anwender sich dringend besser schützen müssen. Nicht erst die Vorfälle der letzten Wochen zeigen, dass ein sicherer Zugangsschutz zu den genutzten Online-Diensten ein absolutes Muss ist. Doch ein starkes Passwort allein reicht nicht aus. Auch die Diensteanbieter sind in der Pflicht, die Daten ihrer Kunden besser zu schützen. Dazu müssen sie sichere Zugangsverfahren wie etwa eine Zwei-Faktor-Authentisierung anbieten und ihre eigenen Anwendungen noch besser gegen Cyber-Kriminalität schützen. Das BSI als die nationale Cyber-Sicherheitsbehörde wird diese Ansätze im Rahmen des Digitalen Verbraucherschutzes mit Nachdruck gegenüber den Anbietern verfolgen und die Unterstützungsangebote für Anwenderinnen und Anwender weiter ausbauen“, betont BSI-Präsident **Arne Schönbohm**.

„Es gibt keinen 100-prozentigen Schutz vor Kriminalität im Internet. Die Tricks und Maschen der Betrüger sind ausgefeilt und perfide. Daher appellieren wir als Polizei an jeden Betroffenen und jede Betroffene sich bei einem Schaden an die Polizei zu wenden. Ihre Anzeige ist entscheidend, um Täter zu verfolgen“, sagt **Gerhard Klotter**, Vorsitzender der Polizeilichen Kriminalprävention der Länder und des Bundes. „Jede Anzeige ermöglicht der Polizei auf aktuelle Vorgehensweisen schnell zu reagieren und Bürgerinnen und Bürger zeitnah zu warnen.“

Es gibt viele Wege, wie Cyber-Kriminelle an die Daten der Internetnutzer kommen können. Mittels Phishing versuchen Betrüger die Anwender dazu zu verleiten, ihre Daten selbst herauszugeben. Zudem können über Schadprogramme wie Trojaner Zugangsdaten gestohlen werden. Hacker überwinden schwache Passwörter mit automatisierten Verfahren. Deswegen zeigen BSI und die Polizei gemeinsam Wege auf, wie sich jeder Einzelne schützen kann.

Phishing und Schadsoftware per E-Mail

Als seriöse Bank oder Firma getarnt, schöpfen Betrüger Passwörter, Kreditkarten- und Kontoinformationen oder PIN / TAN für das Online-Banking ab.

- Überprüfen Sie Ihre Nachrichten mit dem 3-Sekunden-Sicherheits-Check: Achten

PRESSEKONTAKT

PROGRAMM POLIZEILICHE KRIMINALPRÄVENTION der Länder und des Bundes (ProPK)
ZENTRALE GESCHÄFTSSTELLE
c/o LKA Baden-Württemberg
Taubenheimstraße 85
70372 Stuttgart
Telefon (0711) 54 01-20 62
presse@polizei-beratung.de

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK
PRESSESTELLE
Godesberger Allee 185-189
53175 Bonn
Tel.: (0228) 999582-5777
E-Mail: presse@bsi.bund.de

Sie auf Absender, Betreff und Anhänge und ob diese Ihnen plausibel erscheinen.
- Nutzen Sie einen Anti-Viren-Scanner, um mögliche Schadprogramme zu entfernen.
- Führen Sie Updates immer automatisch durch.

Datenleaks und Doxing

Beim so genannten Doxing sammeln Täter personenbezogene Daten, die sie bündeln und öffentlich verfügbar machen. Die beste Vorbeugung ist der sparsame Umgang mit den eigenen Daten im Internet. Zudem sollten Diensteanbieter nach Seriosität und angebotenen Sicherheitseigenschaften ausgewählt werden.

- Nutzen Sie starke Passwörter, vor allem für Zugänge zu Kunden-Accounts bei Banken, Online-Shops, sozialen Medien und für E-Mail-Postfächer.
- Aktivieren Sie eine Zwei-Faktor-Authentisierung bei passwortgeschützten Anwendungen.
- Passwortmanager können eine hilfreiche Unterstützung sein.

Sofort reagieren bei Datenklau

Personen, deren sensible Daten öffentlich gemacht oder für andere Zwecke missbraucht wurden, müssen umgehend reagieren:

- Überprüfen Sie, von welchen Konten Ihre Daten abgegriffen wurden.
- Setzen Sie die Konten zurück und wählen Sie starke Passwörter. Beginnend mit den Accounts, die für das Zurücksetzen von Passwörtern in anderen Anwendungen notwendig sind (z.B. E-Mail-Konten). In einem zweiten Schritt setzen Sie Online-Profile wie Facebook zurück, weil Sie sich mit diesem Account bei anderen Diensten anmelden können.

Jede Straftat anzeigen

Opfer von Cybercrime sollten jede Straftat bei der Polizei anzeigen. Eine Strafanzeige kann bei jeder Polizeidienststelle erstattet werden. Existierendes Datenmaterial – wie E-Mails, Chat-Verläufe in Messenger-Diensten, digitale Fotos oder Videos – sind wichtige Beweismittel, die Sie bis zum ersten Kontakt mit der Polizei bestenfalls komplett unverändert lassen.

Es gibt weitere Wege, wie die Cyber-Kriminellen an sensible Daten kommen. Im Februar stellen die Polizei und BSI für Bürger auf ihren Websites beispielhaft Fälle vor.

BSI für Bürger: www.bsi-fuer-buerger.de
ProPK: www.polizei-beratung.de

Weiterführende Informationen zum Grundschutz gibt der Sicherheitskompass: https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/sicherheitskompass/

Diese Pressemitteilung sowie weitere Informationen finden Sie im Internet unter: www.polizei-beratung.de/presse und www.bsi.bund.de/presse

PROFIL PROGRAMM POLIZEILICHE KRIMINALPRÄVENTION

Das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) verfolgt das Ziel, die Bevölkerung, Multiplikatoren, Medien und andere Präventionsträger über Erscheinungsformen der Kriminalität und Möglichkeiten zu deren Verhinderung aufzuklären. Dies geschieht unter anderem durch kriminalpräventive Presse- und Öffentlichkeitsarbeit und durch die Entwicklung und Herausgabe von Medien, Maßnahmen und Konzepten, welche die örtlichen Polizeidienststellen und andere Einrichtungen, zum Bei-spiel Schulen, in ihrer Präventionsarbeit unterstützen.

PROFIL BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Als neutrale Stelle befasst sich das BSI mit allen Fragen zur IT-Sicherheit in der Informationsgesellschaft. Neben der IT-Sicherheit der Bundesverwaltung bilden insbesondere die Beratung, Sensibilisierung und Aufklärung der Bürgerinnen und Bürger sowie die Kooperation mit Wirtschaft und Wissenschaft hierbei Arbeitsschwerpunkte.