koeln.polizei.nrw.de

POLIZEI
Nordrhein-Westfalen
Köln

bürgerorientiert · professionell · rechtsstaatlich

Computereinbruch
Handeln ist erforderlich!

Parallelen

Nach einem Einbruch ist Ihr Handeln erforderlich. Professionell handelnde Täter richten oft und zunächst unbemerkt Schaden an. Im Haus, der Wohnung und so auch in der digitalen Welt, im Computer.

Zu Ihrer Sicherheit:
Smartphones, Tablets, Notebooks, Smart-TV, PC… Nach einem Einbruch in Ihren Computer sollten Sie aufräumen, wie Sie es nach einem Einbruch in Ihr Haus oder in Ihre Wohnung auch tun würden.

Täter spähen aus

Sie suchen ein geeignetes, schwaches Ziel, wie eine schlecht oder ungesicherte Tür.

Wohnungen/Häuser haben viele Türen und Fenster, durch die eingebrochen werden kann.

Computer haben genau 65536 Türen (Ports), die unterschiedlich gesichert sind.

Täter brechen auf

Sie dringen durch nicht ausreichend gesicherte Türen und Fenster ein.

Ebenso auch bei nicht ausreichend gesicherten Rechnern. Täter nutzen „Bugs“ (Fehler in der Software), die sie mit Programmen feststellen können, wenn der Computer eingeschaltet und mit dem Internet verbunden ist. Und das von irgendwo auf der Welt.

Täter suchen nach Beute

Sind die Täter erst einmal „drin“, sehen sie sich um.

Sie durchsuchen Schränke, Tresore und vermutete Verstecke nach Dingen, die sie als Beute mitnehmen möchten.

Im Rechner bewegen sich die Täter virtuell. Erforschen die Umgebung, spionieren, suchen nach „Schlüsseln“ (zum Beispiel Passwörtern).

Täter nehmen weg

Sie stehlen oft Schmuck, Bargeld, Ausweise, Autoschlüssel, Bank- und Gesundheitskarten.

In den Datenspeichern öffnen sie Datentresore und stehlen Geheimnisse. Sehen in Datenbanken nach, um etwas über den/die Besitzer zu erfahren. Stehlen Fotos und digitale Dokumente. Sie brechen mit den gestohlenen Passwörtern in Profile, E-Mail-Konten oder Shops ein.

Täter schaffen Unordnung oder zerstören

Sie durchwühlen Schrankinhalte, Schmuckkästen, Geldkassetten und lassen nicht gewollte Inhalte achtlos auf die Erde fallen.

Sie verschlüsseln Daten, sperren den Eigentümer aus, löschen und verändern Daten. Sie überfordern die Rechnerleistung und bringen Server zum Stillstand oder Absturz. Sie legen Abläufe oder die Produktion lahm, erpressen und bauen Fallen sowie Spionageprogramme ein.

Täter werden bemerkt

Die Polizei wird aufmerksam und eilt zur Hilfe.

Das Schutzprogramm stellt einen Virus, ein Schadprogramm fest.

Täter werden im Idealfall festgenommen

Die Polizei nimmt Täter fest und führt sie dem Richter vor.

Das Schutzprogramm legt das Schadprogramm in die Quarantäne – sperrt es ein oder löscht es.

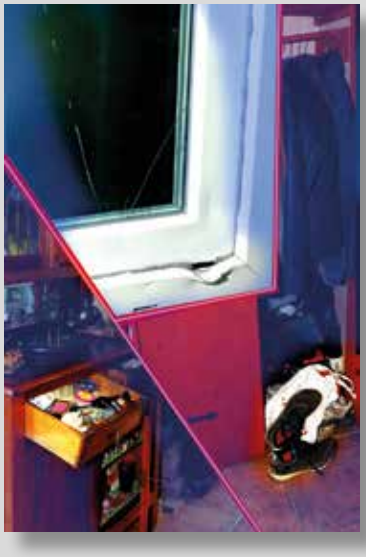
Täter machen „heute“ keine Beute

Die Polizei findet das Diebesgut und gibt es zurück.

Die Schutzprogramme haben dafür gesorgt, dass die Daten nicht gelöscht oder verschlüsselt werden.

Was bleibt, ist der Schaden!

Die Polizei repariert nicht die verursachten Schäden.



Die vom Täter aufgebrochenen Türen, Fenster und die geschaffene Unordnung und Zerstörung bleiben.

Die Schutzsoftware repariert nicht den Computer. Täter halten sich Türen auf (Backdoors). Weitere Schadprogramme wurden unbemerkt installiert. Das Betriebssystem wurde stark beschädigt.

Nur durch eine Neuinstallation des Betriebssystems können Sie nach einem Angriff wieder einen sicheren Zustand Ihres Computers herstellen.

Das können Sie tun!

- Informieren Sie sich.
- Nutzen Sie das Internet mit wachem Verstand.
- Sparen Sie mit Ihren Daten.
- Nutzen Sie Schutzsoftware und nur aktuelle Betriebssysteme.
- Sorgen Sie für Datensicherung.
- Nutzen Sie das Internet nur dort, wo es nötig ist.
- Helfen Sie anderen Nutzern, die Schwierigkeiten haben.
- Lassen Sie sich von Ihrer Polizei beraten.

Herausgeber:
Polizeipräsidium Köln
Walter-Pauli-Ring 2-6
51103 Köln
koeln.polizei.nrw.de
poststelle.koeln@polizei.nrw.de

Fachverantwortung:
Direktion Kriminalität
Kriminalkommissariat Kriminalprävention/Opferschutz
Cybercrime

Tel. 0221 229-8655

Stand: 10/2016