Bedrohungen durch Schadsoftware



Durch den Datenaustausch mit verschiedenen Datenträgern, im Intranet und nicht zuletzt durch die Benutzung des Internets können Schadprogramme in einen PC oder andere elektronische Geräte eindringen. Diese Schadprogramme können Dateien beschädigen, löschen oder unbrauchbar machen. Sie könnten sich unberechtigten Zugang zum System verschaffen und dadurch Daten ausspionieren oder sogar den PC lahmlegen. Aber auch harmlose, unerwünschte E-Mails (Spam) können Mailserver und Benutzerpostfächer erheblich belasten und zu zusätzlichen Kosten und Zeitverlust führen.

Aus diesem Grund ist es für den Benutzer elektronischer Daten- und Informationsquellen wichtig zu wissen, welche Gefahren dadurch drohen und wie diese sich verbreiten bzw. wie man sich gegen diese Gefahren schützt.

Quellen von Bedrohungen

Datenträger

Das Ausführen von Dateien mit schädlichem Code von einem Datenträger (CD, DVD, Disketten, Speicherkarten, USB-Speicher) kann zur Beschädigung des eigenen Computers führen und, ist der Computer mit einem Netzwerk verbunden, auch in der Ausbreitung der Schadsoftware auf andere Computer im Netzwerk resultieren. Diese werden infiziert und zum Beispiel angreifbar für Hacker gemacht.

Internet

Webseiten oder vermeintlich „kostenlose“ Software sind die Hauptverbreitungsquellen für Viren und Schadsoftware. Skripts, werden durch das Öffnen von Webseiten automatisch im Hintergrund ausgeführt. Diese können unter anderem zu Datendiebstahl, Manipulation der Systemregistrierung oder der Installation von schädlichen Programmen führen.

E-Mails

Schadprogramme, die als Anhang einer E-Mail oder direkt in der E-Mail platziert sind, infizieren den Computer beim Öffnen der E-Mail oder beim Speichern des Anhangs. Außerdem bieten E-Mails eine weitere Bedrohung durch „Phishing“, dem Ausspionieren von vertraulichen Informationen.

Typen von Bedrohungen

Je nach Aktion und Gefährdungsgrad lassen sich verschiedenen Typen unterscheiden, wobei oft auch Mischformen vorkommen.

Würmer

Ihren Namen haben Würmer, weil sie Schwachstellen von Betriebssystemen nutzen und sich von Computer zu Computer “wurmartig“ verbreiten. Sie ermitteln Netzwerkadressen oder verwenden Adressbücher von Mailprogrammen und versenden sich selbständig. Sie erreichen dabei eine hohe Verbreitungsgeschwindigkeit.

Viren

Im Gegensatz zu Würmern verbreiten sich Viren nicht selbständig, sondern werden erst durch eine Aktion des Benutzers, z. B. das Kopieren einer verseuchten Datei auf das System und Ausführen der Datei oder des Programmes, aktiv.

Trojanische Programme

Dies sind Programme, die vom Benutzer unbemerkt Aktionen wie das Löschen, Modifizieren, Kopieren und Sperren von Dateien ausführen und damit die Funktionalität des Computers beeinflussen. Im Gegensatz zu Würmern verbreiten sich Trojaner nicht selbständig. Zu diesen Programmen zählen unter anderem Backdoor, Exploit und Rootkits.

Backdoor

Mit einem Backdoor-Trojaner kann der Angreifer die Kontrolle über einen Computer übernehmen und auf diesem beliebige Aktionen, wie das Starten von Programmen, Kopieren und Löschen von Dateien usw., durchführen oder den Computer für kriminelle Zwecke nutzen.

Exploit

Diese Programme werden eingesetzt, um Schwachstellen und Sicherheitslücken einer Software auszunutzen und damit zum Beispiel Nutzerdaten auszulesen. Exploit werden auch gezielt für Spionage und Abhöraktionen genutzt.

Rootkits

Diese werden dazu genutzt, um Schadprogramme vor dem Nutzer und Antivirenprogrammen zu verstecken.

Spyware

Diese Software erlaubt es, Informationen über Benutzer und damit über Organisationen zu sammeln. Es werden Benutzeraktionen überwacht, Festplatteninhalte gescannt oder Informationen über Surfverhalten und Internetverbindungen gesammelt. Darunter fallen auch Keylogger, die Tastatureingaben kontrollieren und andere Aktivitäten des PC-Nutzers überwachen und damit z. B. Passwörter ausspionieren.

Spam

Der Versand von unerwünschten Informationen über das Internet wird als Spamming bezeichnet. Dies verursacht Kosten durch die zusätzlich anfallenden Datenmengen, aber auch durch Arbeitszeit, die zum Ausfiltern von Spam aufgewendet wird bzw. auch für die Anschaffung von Spamfiltern. Mit Spam-E-Mails werden auch Mails versandt, die es zum Ziel haben, Geld zu „erschleichen“, Computer mit Schadsoftware zu infizieren (z. B. Trojaner-Software) oder Phishing-Kampagnen durchzuführen.

Phishing

Beim sog. Phishing werden über E-Mails oder Webseiten durch die Gutgläubigkeit der Benutzer Informationen gesammelt, die zu Identitätsdiebstahl und in weiterer Folge zum Beispiel zu Kontoplünderungen führt. Oft werden E-Mails von Banken oder Kreditkarten-Unternehmen versandt, mit der Bitte um Abgleich der persönlichen Daten durch Eingabe von Benutzername und Passwort. Dies fällt auch unter den Begriff Social Engineering.