Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Leitfaden

Bedrohung der Informationssicherheit durch den gezielten Einsatz von Schadprogrammen

Teil 1: Gefährdungen und Maßnahmen im Überblick

Teil 2: IT-Sicherheitsmaßnahmen gegen spezialisierte Schadprogramme

Teil 3: Kurztest zur Einschätzung der eigenen Bedrohungslage

Thema

Die Bedrohung von schützenswerten Informationen hat durch die Weiterentwicklung von Schadsoftware eine neue Dimension erreicht. Dieser Leitfaden beschäftigt sich in erster Linie mit Schadprogrammen, die individuell für ein bestimmtes Opfer geschrieben werden und maßgeschneiderte Funktionen bieten. Sie sind besonders gefährlich, da sie von klassischen Viren-Schutzprogrammen und Firewalls nicht mehr zuverlässig erkannt werden können.

Da Spionageprogramme zunehmend aus kriminellen oder nachrichtendienstlichen Motiven gegen Behörden und Unternehmen eingesetzt werden, ist eine Anpassung und Erweiterung bestehender Sicherheitskonzepte notwendig.

Aufbau und Zielgruppe

Der Leitfaden besteht aus drei Teilen:

1. Der erste Teil erläutert die Wirkungsweise moderner Schadprogramme, stellt das Gefahrenpotential dar und gibt einen Überblick über mögliche Sicherheitsmaßnahmen. Er richtet sich an **Führungskräfte** mit Zuständigkeit für Informationstechnik und Informationssicherheit, **IT-Sicherheitsbeauftragte** und interessierte **IT-Anwender.** Zum Verständnis ist allgemeines IT-Wissen von Vorteil.

2. Der zweite Teil beschreibt konkrete Maßnahmen und richtet sich an **IT-Sicherheitsbeauftragte** und **IT-Personal** mit guten technischen Kenntnissen. An vielen Stellen werden weitere Informationsquellen wie Studien, Best-Practice-Ratgeber oder Standards angegeben, die bei der praktischen Umsetzung der Maßnahmen hilfreich sind.

   Es gibt zurzeit *kein einzelnes* Sicherheitsprodukt, das einen ausreichenden Schutz gegen individuell angepasste Schadprogramme bietet. Es wird auch jeder Versuch scheitern, *die wichtigste* Maßnahme zu benennen. Einem Angreifer stehen vielfältige Techniken und Informationen zur Verfügung, um in fremde Rechner einzudringen. Ihm genügt eine einzige Schwachstelle im Programmcode einer Anwendung, in Konfigurationsdateien oder im Design einer IT-Landschaft. Sicherheitsmaßnahmen müssen daher ein breites Spektrum abdecken - vom Schutz einzelner Rechner über organisatorische Maßnahmen, die Ausbildung der Mitarbeiter bis zur Netzsicherheit. Dieser Leitfaden hilft bei der Auswahl wirksamer Sicherheitsmaßnahmen und gibt Hinweise, wo Standardmaßnahmen durch höherwertige ergänzt werden müssen.

3. Den dritten Teil bildet ein Kurztest zur Einschätzung der eigenen Bedrohungslage durch gezielte Angriffe mit Schadprogrammen. Das Ergebnis gibt **Führungskräften** einen ersten Anhaltspunkt, wie gut vertrauliche Informationen geschützt sind und wie wahrscheinlich es ist, durch Spionage oder Sabotage Schaden zu nehmen.