Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Leitfaden

Bedrohung der Informationssicherheit durch den gezielten Einsatz von Schadprogrammen

Teil 3: Kurztest zur Einschätzung der eigenen Bedrohungslage

Änderungshistorie

Datum	Änderung
22.01.2007	Version 1

Ansprechpartner

Referat 113 - VS- und IT-Sicherheitsberatung

E-Mail: Referat113@bsi.bund.de

Tel.: +49 (0) 22899-9582-5220

Referat 125 - IT-Penetrationszentrum, Abwehr von Internetangriffen

E-Mail: Referat125@bsi.bund.de

Tel.: +49 (0) 22899-9582-5304

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: http://www.bsi.bund.de

Thema und Zielgruppe

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.

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.

1 Anleitung

Sinn und Zweck

Der Kurztest hilft bei der Einschätzung der eigenen Bedrohungslage durch gezielte Angriffe mit Schadprogrammen:

- Wie gut sind vertrauliche Informationen geschützt?
- Wie wahrscheinlich ist es, durch Spionage oder Sabotage Schaden zu nehmen?

Der Kurztest geht von einer typischen, vernetzten IT-Landschaft aus und bewertet das Risiko, durch einen gezielten Spionage- oder Sabotageangriff mit Schadprogrammen (z. B. Trojanischen Pferden) Schaden zu nehmen. Die Maßnahmen gehen über ein mittleres IT-Sicherheitsniveau hinaus, da sich der Leitfaden hauptsächlich an Behörden und Unternehmen richtet, die besonders schützenswerte Informationen verarbeiten und von professionellen Angreifern bedroht werden.

Die Gewichtung der einzelnen Maßnahmen folgt ihrer Wirksamkeit bei der Abwehr speziell angepasster Angriffssoftware. Ein Fragebogen zum Schutz vor „gewöhnlichen" Attacken aus dem Internet würde daher anders aussehen. Beispielsweise bringt ein lokales Viren-Schutzprogramm nur wenig Pluspunkte, da es kaum vor gezielten Angriffen schützt und als allgemein bekannte Sicherheitsmaßnahme überall zum Standard gehört.

Der Kurztest ist keine vollständige Checkliste und gibt lediglich einen ersten Eindruck über das eigene Risiko. Während bei niedrigen Punktzahlen und entsprechender äußerer Bedrohung ein dringender Handlungsbedarf besteht, darf eine hohe Punktzahl nicht überinterpretiert werden. Bereits eine einzige Schwachstelle kann einem Angreifer ausreichen, um Zugang zu vertraulichen Informationen zu erhalten.

Es ist auf jeden Fall ratsam, mit Hilfe des Leitfadens eine intensive Risikobetrachtung vorzunehmen und das eigene IT-Sicherheitskonzept kritisch zu überprüfen.

Durchführung

Beantworten Sie die folgenden Fragen und addieren Sie bei einer positiven Antwort die Punkte. Die Punkte dürfen nur vergeben werden, wenn alle Teile einer Frage mit „ja" beantwortet werden können.

Eine Ausnahme bildet Frage 7: Hier werden bei einem „nein" 5 Punkte abgezogen.

2 Fragebogen

Schulung und Sensibilisierung der Mitarbeiter

Fragen	Punkte
1 Gibt es spezielle Schulungen zur IT-Sicherheit für alle Mitarbeiter? Folgende Themen müssen behandelt werden: E-Mail- und Internetsicherheit, Umgang mit Datenträgern sowie Social-Engineering-Methoden Werden die Mitarbeiter zusätzlich durch konkrete Maßnahmen sensibilisiert?	2

IT-Management

Fragen		Punkte
2 Umgang mit Schwachstellen	Werden wichtige Sicherheitsupdates unverzüglich eingespielt? Werden umgehend IT-Anwendungen oder Dienste abgeschaltet oder zumindest durch zusätzliche Maßnahmen gesichert, wenn eine gefährliche Schwachstelle veröffentlicht wurde, aber noch kein Patch zur Verfügung steht?	2
3 Zentrale Administration	Werden alle IT-Systeme zentral von speziell geschultem Personal nach einheitlichen und schriftlich festgehaltenen Richtlinien administriert und gewartet? Sind die Rechte der IT-Anwender beschränkt?	2

Absicherung von Arbeitsplatz-Rechnern

Fragen		Punkte
4 Desktop-Firewalls	Sind auf allen Arbeitsplatz-Rechnern lokale Desktop-Firewalls installiert?	3
5 Öffnen von Office-Dateien	Werden unbekannte Office-Dateien (z. B. Word, Excel, Powerpoint) aus fremden Quellen von den Mitarbeitern zunächst mit speziellen Datei-Viewern geöffnet, die nicht makrofähig sind?	2
6 Virenschutz	Ist jeder Arbeitsplatz-Rechner mit einem Viren-Schutzprogramm ausgestattet, das zentral installiert und gewartet wird? Zentrale Wartung schließt ein, dass ein Administrator bemerken würde, wenn das Viren-Schutzprogramm auf einem Arbeitsplatz-Rechner nicht aktiv ist oder die Signaturen veraltet sind.	2

Vernetzung und Internet

Der Fragebogen berücksichtigt nicht alternative oder individuell abgesicherte Internetnutzungsmöglichkeiten über Terminalserver, mit Virtualisierungssoftware oder die Verwendung von Whitelists mit erlaubten Kommunikationspartnern. Sollten diese oder ähnliche Techniken bei Ihnen zum Einsatz kommen, sollte die Punktevergabe individuell angepasst werden. So kann eine Terminalserverlösung die gefahrlose Nutzung von Aktiven Inhalten ermöglichen. In diesem Fall wären dann bei Frage 9 ebenfalls 5 Punkte angemessen.

Fragen		**Punkte**
7 Verarbeitung von besonders schützenswerten Informationen	Werden besonders schützenswerte Informationen nur auf Systemen ohne Internetanschluss verarbeitet (z. B. Standalone-System oder speziell gesichertes internes Netz? Besonders schützenswert bedeutet in diesem Zusammenhang zum Beispiel: Der Verlust der Vertraulichkeit oder Sabotage kann die Existenz eines Unternehmens bedrohen, hat Auswirkungen für die Sicherheit der Bundesrepublik Deutschland oder ein enormer Schaden könnte entstehen.	ja: +0 nein: -5
8 Sicherheitsgateway	Wird an der Schnittstelle zum Internet eine dreistufige Firewall (Paketfilter, Application-Level-Gateway, Paketfilet) betrieben?	2
9 Aktive Inhalte	Werden Aktive Inhalte (ActiveX, Javascript, Active Scripting, Java) bei der Kommunikation mit externen Partnern geblockt?	5
10 Download von ausführbaren Dateien	Werden das Herunterladen von ausführbaren Dateien aus dem Internet und der Empfang von ausführbaren E-Mail-Anhängen technisch verhindert?	3
11 Absicherung von SSL	Werden SSL-Verbindungen zu externen Servern abgesichert (z. B. Zugriff nur über einen SSL-Proxy)? Zentrale Schutzprogramme können verschlüsselte Kommunikationsverbindungen nicht überwachen. SSL-Verbindungen können daher zum unerkannten Einschleusen von Schadprogrammen wie zum heimlichen Herausschleusen von vertraulichen Informationen missbraucht werden.	1
12 Zentraler Virenschutz	Werden zentral alle Kommunikationswege und Protokolle (auch HTTP) überwacht?	1

Gesamtpunkte:	

3 Ergebnis

Begriffsbestimmung und Legende:

- Ein Angriff auf **besonders schützenswerte Informationen** kann schwerste Schäden zur Folge haben (oder Sabotage). Beispiele: Der Verlust der Vertraulichkeit kann die Existenz eines Unternehmens bedrohen oder hat Auswirkungen für die Sicherheit der Bundesrepublik Deutschland, durch Sabotage können Menschen schwer geschädigt werden.

- Ein Angriff auf **wichtige Informationen** kann hohe, aber nicht Existenz bedrohende Schäden zur Folge haben.

- Ein „**Risiko“** ist die Vorhersage eines möglichen Schadens und wird durch die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens berechnet.

☺|😐|☹: Es besteht kein erhöhtes Risiko. | Es ist Vorsicht geboten. | Es besteht ein hohes Risiko.
Rot steht für „besonders schützenswerte Informationen“, Gelb für „wichtige Information“.

Punktzahl	Risikoeinschätzung
21-25 ☺ | ☺	Um Ihre Sicherheitsmaßnahmen zu überwinden, ist ein sehr hoher Aufwand erforderlich. Ein erfolgreicher Angriff ist daher unwahrscheinlich. Um dennoch erfolgreich zu sein, wird ein Angreifer wahrscheinlich unveröffentlichte Software-Schwachstellen suchen, besonders ausgefeilte Social-Engineering-Methoden anwenden oder einen Innentäter anwerben. Es besteht kein erhöhtes Risiko bei der Verarbeitung besonders schützenswerter Informationen.
16-20 ☹ | ☺	Ein erfolgreicher Angriff benötigt hohe Motivation und Geduld, ist aber nicht unmöglich. Der Aufwand ist hoch und setzt spezielles Know-how voraus. Besonders schützenswerte Informationen sollten mit weitergehenden Maßnahmen geschützt werden, wenn eine konkrete Bedrohung durch Spionage oder Sabotage besteht. Die Verarbeitung wichtiger Informationen ist ohne hohes Risiko möglich.
10-15 ☹ | 😐	Entsprechend motivierte Angreifer haben eine realistische Chance, vertrauliche Daten auszuspähen oder zu verändern. Ein Angreifer mit gutem IT-Know-how benötigt höchstens drei Monate, um erfolgreich zu sein. Wenn hoch vertrauliche Daten verarbeitet werden, sollte genau überlegt werden, ob eine äußere Bedrohung durch Spionage oder Sabotage besteht. Ist dies der Fall, sollten zusätzliche Sicherheitsmaßnahmen überlegt werden. Eine Verarbeitung von wichtigen Informationen sollte nur erfolgen, wenn keine besondere Bedrohung von außen besteht, ansonsten besteht ein hohes Risiko.

5-9 ☹ | ☹	Gezielte Spionage- oder Sabotageangriffe sind ohne großen technischen Aufwand durch Angreifer mit durchschnittlichem Know-how durchführbar. Ein Schaden durch „gewöhnliche“, ungezielte Angriffe aus dem Internet kann nicht ausgeschlossen werden. Es besteht die Gefahr, dass Sie zufällig von kriminellen Organisationen angegriffen werden. Ihre Rechner lassen sich z. B. zum Spam-Versand missbrauchen, oder Online-Transaktionen (z. B. Online-Banking) können zunächst unbemerkt manipuliert werden. Die IT-Landschaft ist zur Verarbeitung wichtiger Informationen ungeeignet.
-5 - +4 ☹ | ☹	Ihre Daten stehen jedem Angreifer praktisch offen. Der Aufwand, um wichtige Informationen einzusehen ist gering.