Ganzheitliche Architektur zur Entwicklung und Analyse sicherheitskritischer Systeme und Anwendungen

Mario Golling, Robert Koch, Peter Hillmann und Gabi Dreo Rodosek

Lehrstuhl für Kommunikationssysteme und Internet-Dienste
Fakultät für Informatik
Werner-Heisenberg-Weg 39
Universität der Bundeswehr München
D-85577 Neubiberg
{mario.golling, robert.koch, peter.hillmann, gabi.dreo}@unibw.de

Abstract: Die Forschung auf dem Gebiet der IT-Sicherheit - hier im Speziellen im Bereich der Analyse von Malware sowie gezielten Angriffen - stellt besondere Anforderungen an den Aufbau und den Betrieb von IT-Systemen. Um Informationen über Angriffsmuster und Angreiferverhalten zu erlangen, muss potentiellen Angreifern ein attraktives Ziel geboten werden, das nach außen hin den Anschein eines realen Produktivsystems bzw. -netzes erweckt und sich entsprechend verhalten muss. Sollen über eine Analyse von automatisiert arbeitender Schadsoftware hinaus Aktivitäten professioneller Angreifer analysiert werden, reicht die ausschließliche Nutzung herkömmlicher Honeypots nicht aus. Gleichzeitig allerdings muss sichergestellt werden, dass alle mit einem Angriff verbundenen Aktionen protokolliert und ein Übergreifen des Angriffs aus der Forschungsumgebung auf die produktiven Bereiche verhindert wird.

Probleme bei Untersuchungen in diesem Bereich bestehen in der vollständigen Verhinderung von übergreifenden Angriffen auf die stetig laufenden Produktivsysteme und somit in der Gefahr selbst Opfer zu werden. Im Gegensatz dazu sollte die einzurichtende Testumgebung nach außen hin wie ein reales Produktivnetz aussehen und verhalten, um die Echtheit zu gewährleisten. Aus diesem Grund wäre es ungünstig ein separates Netz ohne produktive Systeme dafür herzunehmen. Weiterhin besitzen die meisten Forschungseinrichtungen und Unternehmen nicht die Möglichkeit einen kompletten Netzbereich nur für die Entwicklung und Analyse sicherheitskritischer Systeme einzurichten. Daher wird ein Teil von einem produktiv genutzten Netzbereich für die Forschung an Malware und Analyse von Angriffen deklariert. Dafür ist es zwingend Notwendig, dass entsprechende Sicherheitsvorkehrungen getroffen werden.

1 Einleitung und Problemstellung

Sowohl die Anzahl an Angriffen auf IT-Systeme als auch deren Qualität bzw. Professionalität hat im Laufe der letzten Jahre extrem zugenommen. Klassische Schutzsysteme, wie z. B. Firewalls oder Virenscanner, sind alleine schon lange nicht mehr ausreichend [KSG12]. Angriffe erfolgen heutzutage viel zielgerichteter und sind technisch meist sehr komplex. Eine Konsequenz davon ist, dass traditionelle Honeypots zur Detektion und Analyse von Malware für sich genommen nicht mehr ausreichen, da immer mehr technisch

versierte Angreifer in der Lage sind diese „Fallen“ zu erkennen.

Weiterhin ist es erstrebenswert, bestehende und neu entwickelte Systeme sowie Schutzmechanismen zu Analysezwecken verschiedenen Angriffen unter realen Bedingungen aussetzen zu können. Eine Fragestellung, die in diesem Zusammenhang weiter untersucht werden kann ist z. B. die Fähigkeit verschiedener auf dem Markt erhältlicher Intrusion Detection Systeme (IDS) hinsichtlich der Angriffserkennung sowie der Anzahl und Art der Fehlalarme unter Berücksichtigung absolut gleicher Rahmenbedingungen. So hat sich in der Praxis z. B. wiederholt gezeigt, dass die theoretische Leistung eines IDS unter realen Bedingungen nicht einmal ansatzweise erreicht wird.

Um insbesondere Analysen von gezielten Angriffen durchzuführen (vor allem Angriffsmuster und Angreiferverhalten) sowie Sicherheitsmaßnahmen (z. B. IDS oder Firewalls) testen zu können, ist eine sichere und kontrollierbare Umgebung - in der reale Angriffe wissentlich zugelassen werden - nahezu unerlässlich. Ferner müssen hierzu neben Low- und High-Interaction Honeypots sowie Honeynets (um Angreifer bewusst anzuziehen) auch mit bewussten Sicherheitslücken präparierte Rechnersysteme (in speziell abgesicherten Zonen) betrieben werden.

Diesem Gedanken Rechnung tragend, wird im Rahmen dieser Publikation eine ganzheitliche Architektur zur Entwicklung und Analyse sicherheitskritischer Systeme und Anwendungen vorgestellt, die den hohen, benötigten Schutzbedarf erreicht. Die vorrangige Motivation dabei besteht in der Schaffung einer Forschungsumgebung, welche sich wie ein produktiv genutztes Netz verhält. Das Ziel besteht somit in der Konstruktion einer Architektur für eine sichere und kontrollierbare Forschung innerhalb eines Subnetzes eines ansonsten produktiv genutzten Netzes.

2 Szenario: Analyse von Malware

In diesem Abschnitt soll die Notwendigkeit einer ganzheitlichen Architektur zur Analyse von Malware anhand eines praktischen, realen Szenarios dargestellt werden (siehe Abbildung 1). Die Besonderheit des Szenarios ist der integrative Ansatz unterschiedlichster Komponenten, sowohl von der Angriffserkennung mit Sensoren und Live-Auswertung sowie Korrelation von Daten bis zur Post-Mortem-Analyse für die IT-Forensik. Dabei ist insbesondere hervorzuheben, dass die einzelnen Komponenten dynamisch die Sammlung und Auswertung (Korrelation) der Daten triggern können. Im Folgenden werden die einzelnen Komponenten dargelegt:

2.1 Sensoren

Die Angreifer werden von speziell präparierten Systemen (Clients mit Windows XP, Servern wie Windows 2003 sowie Low-Interaktion und High-Interaktion Honeypots) mit bewusst (simulierten) Schwachstellen von der Forschungsumgebung angelockt. Der Verlauf sowie das Verhalten des Angreifers werden hierbei mehrfach aufgezeichnet - sowohl durch

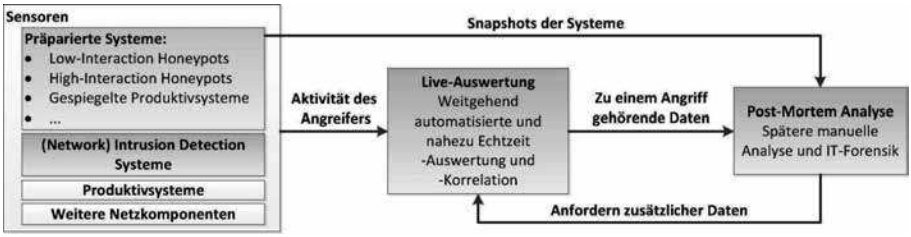

Abbildung 1: Überblick über die verwendete Komponenten

Host- als auch durch Netzkomponenten (Host/Network Intrusion Detection Systeme, Honeypots, Switches mit Monitoring-Port etc.).

2.2 Live-Auswertung

Die Sensoren senden die aufgezeichneten Daten an eine zentrale Datenbank zur Korrelation und Analyse der Aktivitäten der Angreifer. Die generierten Alerts bilden die Grundlage für die weiteren Untersuchungen. Die Auswertung der vielen, generierten Alerts erfolgt dabei zunächst durch eine automatische Korrelation. Dazu existieren bereits verschiedene Konzepte ([CM02], [DW01], [VVKK04]), die allerdings alle Schwachstellen aufweisen und daher im Rahmen der weiteren Forschungsarbeiten verbessert werden sollen. Aktuell werden lediglich die Alerts der IDS, ohne zusätzliche Quellen wie z. B. Honeypots oder Logdaten zur Korrelation einbezogen.

2.3 Post-Mortem Analyse

Für die Rekonstruktion eines Angriffs können anhand vorgegebener Kriterien, z. B. Zeitstempel, Quelle oder Ziel, weitere Daten sowie Snapshots angefordert werden. Dies erweitert die Datenbasis für forensische Untersuchungen. Anschließend könnten mittels entwickelten Maßnahmen über Intrusion Prevention Systemen (IPS) automatisiert Gegenmaßnahmen eingeleitet werden. Als Beispiel wurden zwei Angriffsszenarios untersucht. Das Außentäter-Szenario umfasst einen Angriff aus dem öffentlichen Netz auf die Infrastruktur, um ein Peer-to-Peer Botnetz zu initialisieren. Das Innentäter-Szenario betrachtet einen Angriff aus dem inneren Netz auf das Verwaltungssystem der Universität.

3 Anforderungen

Aus dem beschriebenen Szenario ergibt sich bereits eine Vielzahl von Anforderungen:

- Realisierung einer kontrollierbaren Forschungsumgebung
- Aufzeichnen der Aktivitäten
- Simulation des Produktiv-Verhaltens
- Angriffe von der Forschungsumgebung heraus auf weitere Systeme unterbinden und dennoch gleichzeitig:
  - Minimale und kontrollierte Kommunikation aus der Forschungsumgebung ins Internet (insbesondere zur Analyse des Malwareverhaltens von Botnetzen) zu gestatten
  - Manipulationen von gefährlichen Datenpaketen aus dem Forschungsnetz heraus zu unterbinden
  - Verhinderung der weiteren Verbreitung sowie dem Übergreifen der Angriffe von der Forschungsumgebung auf weitere interne Bereiche
  - Berücksichtigung der gesetzlichen Bestimmungen und eventueller Haftbarkeit
- Unterscheidung von parallel stattfindenden Angriffen
- Mehrstufiges System ineinandergreifender Sicherheitsmaßnahmen
- Notfall Routinen, z. B. Abschalten der Kommunikationsverbindungen über einen separaten Kommunikationskanal (Out-of-Band Kommunikation) [CK10].
- Schutz der Produktivsysteme im Netzbereich
- Vorbereitung von forensischen Untersuchungen

4 Stand der Wissenschaft und Technik

Viele der Rahmenwerke für IT-Sicherheitsarchitekturen (wie ISO27001 oder COBIT) fokussieren insbesondere auf das Management von IT-Sicherheit inkl. der dafür nötigen IT-Sicherheitsprozesse und dem Personal aber weniger auf technische Aspekte und sind daher für diese Publikation als weniger relevant einzustufen (siehe u.a. [Ini01] [Bun09]. Andere Rahmenwerke wie Common Criteria hingegen sind zu stark produktzentriert. Auf dem für diese Veröffentlichung relevanten Gebiet der technisch, architekturbezogenen Forschung (siehe Abbildung 2) sind lediglich die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hervorzuheben, deren Fokus - insbesondere in Form der Grundschutzkataloge - auch in Teilen im technischen Bereich liegt. Somit kommen die Empfehlungen des BSI unseren Anforderungen eines Konzeptes auf technischer Ebene für ganzheitliche Architekturen am nächsten.

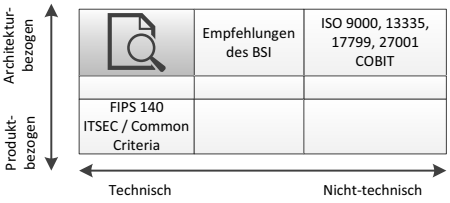

Abbildung 2: Vergleich verschiedener Kriterienwerke zur IT-Sicherheit; adaptiert nach [Ini01]

Empfehlungen des BSI: Der Grundschutzkatalog [Bun11] des BSI bietet Hinweise zur Absicherung von Einzelsystemen über Firewall und Anti-Viren-Schutz für Privatanwender. Die Betrachtung von vernetzten Komponenten wird jedoch weitestgehend vernachlässigt. Für größere IT-Umgebungen bietet das BSI mit den IT-Sicherheitsrichtlinien [Bun11] und dem Leitfaden [Bun12] ein umfassendes Konzept an, wobei beide Dokumente allgemein gehalten sind und konkrete Vorschläge für die Realisierung ausbleiben. Die Beachtung der Vorschriften und gesetzlichen Aspekte wird bei der Umsetzung mit berücksichtigt. Durch den Leitfaden sind erweiterte Ansätze gegeben, welche aber in keiner tiefgreifenden und abschließenden Betrachtung sowie direkten Umsetzung enden.

5 Architektur

Bei der vorgeschlagenen Architektur wird der Datenverkehr aus dem öffentlichen Netz zuerst an spezielle Komponenten weitergereicht, welche den ein- und ausgehenden Datenstrom völlig transparent einfach oder sogar mehrfach duplizieren und die Daten an die Auswerte-Netze für weitere Analysen weiterleiten, aber kein Informationsfluss der Auswerte-Netze nach außen zulassen („Einwege-Verbindung“ bzw. „Datendiode“; im Folgenden *Wire-TAP* genannt); realisierbar z. B. durch Test Access Ports (TAPs) [G$^+$04], SPAN/Mirrorports bzw. mit iptables/netfilter und der Option *Tee* [The13]; siehe Abbildung 3. Danach wird der Datenverkehr, nachdem dieser eine Firewall passiert hat (und entsprechend des dort vorhandenen Regelsatzes gefiltert wurde), über ein oder mehrere Switche (die untereinander über Trunks/Tagged Ports verbunden sind [DS97]) an die Endsysteme weitergeleitet. Die einzelnen Switche wiederum sind - um den Datenverkehr der Forschungsumgebung vollständig auswerten zu können - ebenfalls alle über einen Monitoring-Port an eine zweite Wire-TAP angeschlossen. Das interne Netz letztendlich ist wiederum in einzelne Bereiche gegliedert, die im Folgenden kurz einzeln beschrieben sind:

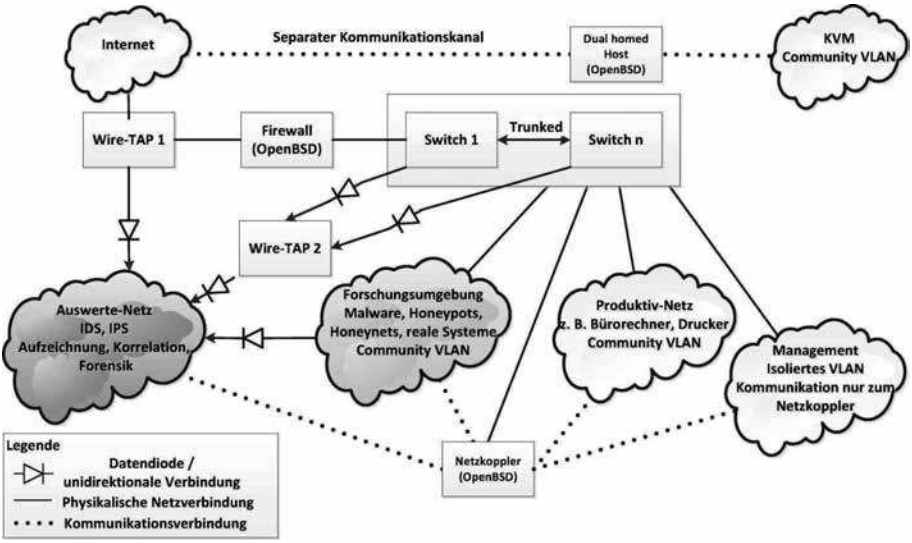

Abbildung 3: Ganzheitliche Architektur zur Entwicklung und Analyse sicherheitskritischer Systeme und Anwendungen

5.1 Forschungsnetz

Dieser geschaffene Bereich dient als Forschungsumgebung zur Überprüfung und Evaluierung der sicherheitskritischen Systeme und Anwendungen. Um entsprechende Angreifer und Malware anzulocken, werden verschiedene Honeypots (wie Honeyd oder Sebek), speziell präparierte Server (Webserver, Datenbankserver, etc.) und Clients sowie im Bedarfsfall auch IPS betrieben. Alle Rechnersysteme in diesem Netz können untereinander kommunizieren und Verbindungen ins öffentliche Netz sind zunächst gestattet. Im Ausgangszustand filtert die Firewall für diesen Bereich des Subnetzes keinen, bzw. nur sehr rudimentär Datenverkehr, um einfacher Malware und Angreifer anzulocken. Falls notwendig, kann - über eine gesonderte Konfiguration der Firewall - eine Fokussierung auf gezielte Angriffe bzw. bestimmte Sicherheitsaspekte erfolgen.

5.2 Produktivnetz

In diesem Teil des Subnetzes befinden sich sämtliche IT-Systeme, welche für den täglichen operativen Betrieb notwendig sind (z. B. Bürorechner und Netz-Drucker). Durch die interne Teilung der Netze bleibt das Verhalten nach außen unverändert, wobei ein Übergreifen von anderen separaten Bereichen auf den Produktivbereich verhindert wird (realisiert durch switchbasierte Sicherheitsfeatures wie feingranulare Access Control Lists (ACLs), Port Security bzw. (Community/Isolated) port-based VLANs [HM03] [Cis08]).

Weiterhin wird durch eine angepasste Konfiguration der Firewall eine weitere Schutzebene eingeführt. Somit ist der in der Praxis entstehende Unterschied bzgl. der Bedrohung durch das Einrichten einer Forschungsumgebung für sicherheitskritische Systeme als gering zu bewerten. Ferner können im Bedarfsfall auch (anonymisierte) Daten aus dem Produktivbereich in die Forschungsumgebung gespiegelt werden, um den Eindruck einer realistischen Infrastruktur zu verstärken. Durch die eingeführten Überwachungssysteme für die Forschungsumgebung können auch die Rechnersysteme im Produktivbereich mit analysiert werden, was zu einem zusätzlich Schutz führt.

5.3 Auswerte-Netz

Für das Auswerte-Netz werden alle Nachrichten der Forschungsumgebung dupliziert (streng genommen sogar mehrfach; sowohl durch die Wire-TAP vor, als auch durch die nach der Firewall). Dadurch wird eine vollständige Überwachung möglich und Alerts können frühzeitig ausgewertet werden sowie als Indikator für aufkommende Bedrohungen dienen. Die IT-Systeme in diesem Teilnetz arbeiten unabhängig von anderen Systemen in weiteren Teilnetzen. Sie erhalten lediglich Informationen aus anderen Netzen, z. B. von der Forschungsumgebung, wobei aber - durch die Wire-TAPs - typischerweise kein rückwärtiger Informationsfluss stattfindet. Innerhalb des Auswertenetzes lassen sich mehrere IDS hingegen direkt verbinden und die Daten verschiedener Auswerte-Systeme können so miteinander korreliert werden. Idealerweise soll dadurch eine Reduzierung der Fehlalarmrate (False-Positives und False-Negatives) als auch eine Steigerung der Erkennungsquote (True-Positives und True-Negatives) erreicht werden. Weiterhin erfolgt eine zentrale Speicherung der Verkehrsdaten (aus datenschutzrechtlichen Gründen in Form von FLOWs [Cla07]) sowie der generierten Metadaten (Alerts, etc.), um beispielsweise zu einem späteren Zeitpunkt den Verlauf eines Angriff nachvollziehen zu können. In der derzeitigen praktischen Umsetzung werden mehrere Server mit gleicher Hardware (Intel P4 2,8 GHz, 2 GB RAM) und Betriebssystem (Ubuntu 10.04.2 LTS, Kernel 2.6.32-30) für die Evaluation der IDS Snort, Suricata, dem kommerziellen Cisco IDS (Cisco IPS 4260) und dem Prelude Framework verwendet. Weiterhin wurde eine zentrale Datenbank für die Speicherung der anonymisierten Daten erstellt.

5.4 Management-Netz

Der separierte Bereich des Management-Netzes dient unter anderem als Kontrollinstanz. Hier findet die Überwachung der verschiedenen Rechnersysteme und Switche statt. Die Verbindung zu den überwachten Systemen erfolgt über ein vom regulären Netzverkehr unabhängiges Netz-Interface an den Servern, welche nur für das Management der Systeme vorgesehen ist. Außerdem lassen sich die Systeme nicht nur kontrollieren und überwachen, sondern auch konfigurieren und managen (wie auch Abbildung 4 verdeutlicht.). Im praktischen Einsatz an der Universität der Bundeswehr München (UniBw) werden hierbei u. a. anderem Nagios und OpenNMS verwendet, um die Rechnersysteme in den ande-

ren Netzen über SNMP überwachen und konfigurieren zu können. Um ein Angriff über das Management-Netz zu verhindern, werden alle Kommunikationsverbindungen bis auf die zum Netzkoppler sowie zu den SNMP-Servern unter Rückgriff auf das Konzept der Community VLANs blockiert [Cis08].

Abbildung 4: Sicherung des Netzes für das Management

5.5 Netzkoppler

Der Netzkoppler ist die zentrale Komponente, um eine netzübergreifende Kommunikationsverbindung herzustellen. Somit ist der Netzkoppler eine sehr sicherheitskritische Komponente, die es gilt im besonderem Maße abzusichern. Um bereichsübergreifende Angriffe über den Netzkoppler zu verhindern, wird die Funktionalität bis auf das absolut Notwendigste eingeschränkt. Dies geschieht zum einen durch Auswahl der Konfiguration des Systems selbst als auch über die Firewall. Aufgrund seiner konsequenten Ausrichtung auf IT-Sicherheit wird für diese sehr sicherheitskritische Komponente an der UniBw OpenBSD eingesetzt [Cow03]. Bei der Installation wurde speziell darauf geachtet, dass nur die absolut notwendigen Pakete verwendet werden. Für die netzübergreifende Kommunikation ist als Dienst einzig OpenSSH mit Public-Key-Authentifizierung aktiviert.

5.6 Keyboard-Video-Mouse

Zur direkten Ansteuerung und Konfiguration der Server und Switche werden mehrere Keyboard-Video-Mouse (KVM) Switche verwendet. Diese ermöglichen die Steuerung mehrerer Rechnersysteme sowie der zentralen Komponenten. Über ein Netzinterface lassen sich die KVMs auch remote ansteuern, sodass eine Fernwartung der verschiedenen Systeme über einen zentralen Einstiegspunkt erfolgen kann (KVM over IP). Der Zugang zu diesem Netz erfolgt - aus Sicherheitsgründen - über einen separaten Kommunikationskanal (out of band communication), um diese Verbindung besonders vor Angriffen zu schützen und eine Konfiguration der Endgeräte unabhängig vom Funktionieren des Rests der Architekturkomponenten auch in besonders gefährlichen Situation zu ermöglichen. Der Zugang ist hier lediglich über einen dual homed Host möglich. An der UniBw wird hier wieder ein Rechner mit einem auf das wesentliche reduzierten OpenBSD (mit OpenSSH und Public-Key-Authentifizierung) benutzt.

6 Erste Erfahrungen

Die ersten Erfahrungen haben gezeigt, dass der Aufbau (physische Verkabelung) und Konfiguration der Architektur im Falle der ersten Inbetriebnahme durchaus diverse Herausforderungen darstellen und im Vorfeld wohl überlegt und durch ein abgestimmtes Migrationskonzept hinterlegt sein sollten, um insbesondere Ausfälle der Produktivumgebung zeitlich auf ein Minimum zu reduzieren.

Die aufwändige Konfiguration der Architektur hat den Angriffen im realen Betrieb standgehalten, obwohl währenddessen verschiedene Sicherheitslücken bekannt wurden, wie z. B. „Multiple Vulnerabilities in Cisco Firewall Services Module“ [Cis12] an dem verwendeten Cisco Firewall-Modul eines Core Switches. Aufgrund der mehrschichtigen Sicherheit, wurden Angriffe in diesem Fall bereits sowohl durch die ACLs der Access-Switche als auch durch die Firewall effektiv blockiert. Somit zeigen die ersten Erfahrungen, dass die Forschungsumgebung eine gute Ausgangsbasis für das Testen und die weitere Entwicklung von Ansätzen zur Angriffserkennung und Malware-Analyse bietet. Das Ergebnis der Analysen zeigte weiterhin, dass insbesondere bei der Wire-TAP vor der Firewall die Verzögerung (Delay) für die Duplizierung der Verkehrsdaten, die die Nutzung eines Switches im Vergleich zu der Nutzung eines physikalischen Netz Taps mit sich bringt, in der Praxis kaum relevant ist (leistungsstarke Backplane vorausgesetzt). Auch die Möglichkeit der Detektion von Fehlern auf den Schichten 1 und 2 (die physikalische Netz Taps im Vergleich zur Nutzung von Switchen bieten) spielt hier praktisch keine Rolle.

7 Zusammenfassung und Ausblick

Der Beitrag zu einer ganzheitlichen IT-Sicherheitsarchitektur für eine kontrollierbare Forschungsumgebung ermöglicht die Forschung an sicherheitskritischen Systemen innerhalb eines produktiv genutzten Netzes. Um die benötigte Sicherheit zu gewährleisten, ist es notwendig bereits beim Design auf der niedrigsten Ebene des Gesamtsystems entsprechende Schutzmechanismen zu integrieren (Security by Design). Somit wird die Sicherheit zum grundlegenden, integralen Bestandteil des Gesamtkonzeptes. Durch die Implementierung weiterer Schutzmaßnahmen auf verschiedenen Ebenen entsteht ein mehrstufiges Sicherungssystem, welches beim Versagen einer Richtlinie dennoch Schutz bietet. Die Architektur erlaubt tiefgreifende Analysen unter realen aber kontrollierbaren Bedingungen.

Literatur

[Bun09] Bundesamt für Sicherheit in der Informationstechnik. *Informationssicherheit: Ein Vergleich von Standards und Rahmenwerken*. Bundesamt für Sicherheit in der Informationstechnik, 2009. `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/studie_ueberblick-standards.pdf?__blob=publicationFile`.

[Bun11] Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutz-Kataloge*. Bundesamt für Sicherheit in der Informationstechnik, 2011. https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf.

[Bun12] Bundesamt für Sicherheit in der Informationstechnik. *Leitfaden Informationssicherheit*. Bundesamt für Sicherheit in der Informationstechnik, 2012. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile.

[Cis08] Cisco Systems. Inc. *Configuring Isolated Private VLANs on Catalyst Switches*. Cisco Systems, 2008. http://www.cisco.com/image/gif/paws/40781/194.pdf.

[Cis12] Cisco Security Advisory. *Multiple Vulnerabilities in Cisco Firewall Services Module*. Cisco Systems, 2012. http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121010-fwsm/.

[CK10] R.A. Clarke und R. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins Publishers, 2010.

[Cla07] B. Claise. *RFC 3954: Cisco Systems NetFlow Services Export Version 9 (2004)*. IETF, 2007. http://www.ietf.org/rfc/rfc3954.txt.

[CM02] F. Cuppens und A. Miège. Alert correlation in a cooperative intrusion detection framework. In *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on*, Seiten 202–215. IEEE, 2002.

[Cow03] C. Cowan. Software security for open-source systems. *Security & Privacy, IEEE*, 1(1):38–45, 2003.

[DS97] P. Draft Standard. 802.1 Q/D10, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, Copyright by the Institute of Electrical and Electronics Engineers, 1997.

[DW01] H. Debar und A. Wespi. *Aggregation and correlation of intrusion-detection alerts. In Recent Advances in Intrusion Detection*, 2001.

[G+04] Network Working Group et al. IETF Policy on Wiretapping. Bericht, RFC 2804, May 2000, 2004.

[HM03] D. Hucaby und S. McQuerry. *Cisco Field Manual: Catalyst Switch Configuration*. Cisco Systems, 2003.

[Ini01] Initiative D21. *IT-Sicherheitskriterien im Vergleich*. Initiative D2, 2001. http://www.rswe.com/Konferenzen/F000176B4/000D1093-70E903AC-000D10B9.0/leitfaden.pdf.

[KSG12] R. Koch, B. Stelte und M. Golling. Attack trends in present computer networks. In *Cyber Conflict (CYCON), 2012 4th International Conference on*, Seiten 1–12. IEEE, 2012.

[The13] The netfilter.org project. netfilter/iptables project homepage, 2013. http://www.netfilter.org/.

[VVKK04] F. Valeur, G. Vigna, C. Kruegel und R.A. Kemmerer. Comprehensive approach to intrusion detection alert correlation. *Dependable and Secure Computing, IEEE Transactions on*, 1(3):146–169, 2004.