Die Umsetzung von Netzsicherheitskonzepten in heterogenen Organisationen

Thomas Schwenkler und Stephan Groß

[1] Fraunhofer Institut Experimentelles Software Engineering,
Sauerwiesen 6, 67661 Kaiserslautern
Thomas.Schwenkler@iese.fhg.de
[2] Technische Universität Dresden,
Fakultät Informatik,
Institut für Systemarchitektur, 01062 Dresden
Stephan.Gross@inf.tu-dresden.de

Zusammenfassung: Die wachsende Abhängigkeit von der Kommunikation über das Internet bei gleichzeitig zunehmender Bedrohung durch immer neue Angriffe stellt auch die Forschungseinrichtungen in Deutschland vor neue Herausforderungen. So lässt sich die Sicherheit der Netzanbindung nicht mehr durch Techniken, wie z.B. Firewalls, alleine lösen. IT-Sicherheit ist vielmehr als Prozess zu verstehen, der von allen Mitarbeitern einer Institution „gelebt" werden muss. Im vorliegenden Artikel stellen wir laufende Arbeiten in der Fraunhofer Gesellschaft zur sicheren Internet-Anbindung der einzelnen Institute vor. Konkret beschreiben wir unsere Erfahrungen bei der Auditierung einzelner Institute nach der Installation des vom Fraunhofer Network Operation Center (NOC) entwickelten Kommunikationsknotens und sich daraus ergebender Konsequenzen für dessen Weiterentwicklung. Hieraus lassen sich Empfehlungen für die Umsetzung von Netzsicherheitskonzepten in heterogenen Organisationen ableiten.

1 Einleitung

Die zunehmende Globalisierung der Informationslandschaft durch das Internet macht eine stete Verfügbarkeit der Informations- und Kommunikationsinfrastruktur für Unternehmen und Forschungseinrichtungen unverzichtbar. Diese ist jedoch permanenten Angriffen ausgesetzt. Insbesondere lässt sich in den letzten Jahren ein Trend weg von einigen wenigen hochspezialisierten Angreifern hin zu einer Vielzahl vollautomatisch durchgeführter Angriffe durch sogenannte Script Kiddies verzeichnen [McH01]. Obwohl diese meist über keine tiefergehenden Systemkenntnisse verfügen, verursachen sie mit immer weniger Aufwand immer größere, mitunter sogar existenzbedrohende Schäden. So wurde beispielsweise im vergangenen Jahr der britische Internet Service Provider Cloud Nine durch eine gezielte Denial-of-Service-Attacke gezwungen, die Geschäftstätigkeit vollständig einzustellen [HON02]. Durch die mittlerweile stark vernetzte und internationale Zusammenarbeit in wissenschaftlichen Einrichtungen wie zum Beispiel der Fraunhofer Gesellschaft (FhG) muss deren Abhängigkeit von einer intakten Internet-Anbindung als mindestens genauso hoch eingestuft werden. Infolge dessen gewinnt der Aspekt der IT-Sicherheit auch hier immer mehr an Bedeutung.

Mit oder gerade als Antwort auf die Veränderungen in der Struktur der beobachteten Angriffe hat sich in den letzten Jahren auch das Verständnis von IT-Sicherheit gewandelt. Wurden bis Ende der neunziger Jahre hauptsächlich technische Maßnahmen zum Schutz der IT-Ressourcen ergriffen, setzt sich seitdem immer mehr die Erkenntnis durch, dass Sicherheit durch Firewalls, Intrusion Detection Systeme usw. alleine nicht erreicht wird. Stattdessen wird IT-Sicherheit vielmehr als aktiv zu lebender evolutionärer Prozess begriffen [Sch00], der die Technik zwar beinhaltet, allerdings mehr auf deren korrekte Nutzung fokussiert. Der IT-Sicherheitsprozess wird dabei in einem ganzheitlichen Zusammenhang gesehen, der von der Planung notwendiger Maßnahmen über deren Realisierung bis hin zum sicheren Betrieb geht.

Wie bereits eingangs erwähnt, sehen sich mittlerweile auch die großen Forschungseinrichtungen in Deutschland wie z.B. die Fraunhofer Gesellschaft, die Max Planck Gesellschaft oder die großen Universitäten mit der geschilderten Sicherheitsproblematik konfrontiert. Als besonders problematisch wirkt sich hierbei der heterogene Aufbau dieser Organisationen aus. So besteht beispielsweise die FhG derzeit aus 57 autonomen Instituten mit Standorten in ganz Deutschland, die mehr als 12.000 Mitarbeiter beschäftigen. Hinzu kommen weltweit noch mehrere Zweigstellen der Fraunhofer Gesellschaft bzw. einzelner Institute. Trotz der Entscheidungsbefugnis der einzelnen Institute muss ein Mindestmaß an Sicherheit für die Kommunikation untereinander gewährleistet werden. Dabei muss man sich vor Augen halten, dass die Gesamtsicherheit immer nur so gut sein kann wie die des schwächsten Glieds in der Kette. Mit anderen Worten, die Sicherheit jedes einzelnen Instituts wirkt sich auf die organisationsweite IT-Sicherheit aus.

Die FhG begegnet dieser Herausforderung mit einem zentral entwickelten Sicherheitskonzept, das durch das Fraunhofer Network Operation Center (NOC) in Form des sogenannten Kommunikationsknotens umgesetzt wird [NOC]. Dieser beinhaltet die von einem Institut zur Bereitstellung der Internet-Konnektivität benötigte Hardware sowie dazugehörige Software bzw. Konfigurationen und stellt einen Mindeststandard für die sichere Netzanbindung in der FhG dar. Die einzelnen Institute dürfen diesen nach Belieben an ihre Anforderungen anpassen oder sogar vollständig durch Eigenentwicklungen ersetzen, wobei die gemachten Änderungen jedoch immer dem vorgegebenen Minimalstandard genügen müssen. Um dies sicherzustellen, ist eine regelmäßige Auditierung der einzelnen Institute unverzichtbar.

Im folgenden beschreiben wir die Ergebnisse einer ersten Auditierungskampagne an ausgewählten Fraunhofer Instituten. Bei der Auswahl wurde der heterogenen Struktur der FhG besondere Bedeutung beigemessen, um möglichst allgemein gültige Aussagen für die Weiterentwicklung des Kommunikationsknotens treffen zu können. Dafür wurden sowohl Institute untersucht, die das vorgegebene Konzept ohne Modifikationen einsetzen, als auch solche, die das Konzept an ihre besonderen Anforderungen angepasst haben oder sogar ein vollständig selbst entwickeltes Konzept verwenden. In Kapitel 2 beschreiben wir zunächst einige allgemeine Überlegungen zum Sicherheitsgrundkonzept und dessen Umsetzung. Anschließend gehen wir näher auf die unterschiedliche Situation der einzelnen Institute in der FhG ein (Abschnitt 3). Kapitel 4 behandelt das Vorgehen bei der Auditierung: Welche Komponenten der Netzanbindung wurden untersucht, wie wurde dabei vorgegangen und welche Werkzeuge wurden dafür verwendet? In Kapitel 5 schließlich

werden die wesentlichen Ergebnisse der Untersuchungen umrissen und mögliche Konsequenzen aufgezeigt, bevor dann in einer abschließenden Betrachtung in Abschnitt 6 ein zusammenfassendes Statement und ein Ausblick auf weitere mögliche Arbeiten gegeben wird.

2 Sicherheitsgrundkonzept

Um innerhalb eines Forschungsverbundes wie der FhG oder einer ähnlichen Einrichtung mit vergleichbar hierarchischer Struktur ein möglichst einheitliches Sicherheitsniveau bei allen Entitäten zu erzielen, bedarf es einer verbindlichen Sicherheitspolitik. Diese beschreibt in allgemeiner Form diejenigen Aktivitäten, die prinzipiell erlaubt bzw. grundsätzlich verboten sein sollen. Die Sicherheitspolitik der FhG wird vom Fraunhofer NOC in Diskussion mit der Fraunhofer Zentralverwaltung und den IT-Verantwortlichen der einzelnen Institute festgelegt. Darauf aufbauend wird ein gesellschaftsweites Sicherheitskonzept erstellt und entsprechend den sich ändernden Randbedingungen der Praxis weiterentwickelt. Dieses Konzept stellt einen minimalen Sicherheitsstandard innerhalb der FhG dar, d.h. jedes Institut ist verpflichtet, für die Einhaltung dieses Sicherheitskonzepts in seinem Umfeld Sorge zu tragen. Es enthält konkrete Anweisungen, wie die vorgegebene Sicherheitspolitik in der Praxis umzusetzen ist. Dafür werden beispielsweise (un-)zulässige Kommunikationsbeziehungen spezifiziert und eine Firewall-Architektur vorgeschlagen.

Um Synergien zu nutzen und jedes Institut unabhängig von den Sicherheitskenntnissen der örtlichen IT-Verantwortlichen in die Lage zu versetzen, dieses Sicherheitskonzept auch auf vertretbare Weise zu realisieren, wird vom Fh NOC darüber hinaus der sogenannte Kommunikationsknoten entwickelt. Dieser umfasst neben der benötigten Standard-Hard- und Software die generischen Konfigurationsdaten zur Implementierung des Sicherheitskonzepts sowie eine eigenentwickelte Konfigurationssoftware, mit der sich der gesamte Knoten über ein „Single Point of Administration“ via Web-Interface warten lässt.

Zur Realisierung ihrer Internet-Anbindung können die einzelnen Institute auf diesen Kommunikationsknoten zurückgreifen. Seine Wartung erfolgt dabei entweder durch den örtlichen IT-Verantwortlichen oder über eine gesicherte Verbindung durch das NOC. Dadurch wird auch Forschungsinstituten ohne ausreichend qualifiziertes Personal eine einfache Möglichkeit zur Einhaltung der vorgegebenen Sicherheitspolitik der FhG angeboten.

Der vom Fh NOC entwickelte Kommunikationsknoten lässt sich im Allgemeinen gut in den Instituten einsetzen, die keine oder nur wenig über die Standarddienste hinausgehende Funktionen für ihre Kommunikationsinfrastruktur benötigen. Mit der IuK-Gruppe befindet sich in der Fraunhofer Gesellschaft aber ein Verbund aus insgesamt 15 Instituten, die auf dem Gebiet der Informations- und Kommunikationstechnik forschen und mit ihren mehr als 2.000 Mitarbeitern den größten Forschungsverbund Europas auf diesem Gebiet bilden. Diese haben typischerweise höhere Anforderungen an die benötigten Netzwerkdienste. Zu dem verfügen die dort arbeitenden Mitarbeiter oftmals über erhebliche eigene Sicherheitskenntnisse, so dass hier ein zwingender Einsatz des Standardkommunikationsknotens nicht zweckmäßig ist, wohl aber die darin verwirklichten Sicherheitsmaßnahmen als Mindeststandard vorausgesetzt werden können.

Die zentral entwickelte Sicherheitspolitik kann also auf Grund der Heterogenität der einzelnen Institute der Fraunhofer Gesellschaft nur einen allgemeingültigen Charakter mit ausreichend Möglichkeiten der Erweiterung und Anpassung besitzen. Sie enthält klare, grundlegende Vorgaben, in denen aber auch bereits die Vielfalt der Bedürfnisse der unterschiedlichen Institute in Form von Ergänzungsmöglichkeiten enthalten ist.

3 Situation der Institute

Trotz einer homogenen Hierarchie in einer Gesellschaft, die ihre Organisationseinheiten nach einheitlichen Standards verwaltet, ist eine Heterogenität bezüglich der Netzanbindung der einzelnen Entitäten nur schwer vermeidbar. Diese Vielfältigkeit führt zwangsweise auch zu teilweise stark unterschiedlichen Anforderungen an die IT-Infrastruktur und das Sicherheitsbedürfnis. Am Beispiel der Fraunhofer Gesellschaft, zu der an mehr als 40 Standorten in Deutschland über 50 Institute gehören, lassen sich dafür zahlreiche Ursachen ermitteln:

- Die Forschungsbereiche der verschiedenen Institute sind unterschiedlich nah an den IT-Bereich angelehnt. Während in einigen Instituten die Vernetzung zwar als unabdingbar, dennoch aber nur als Hilfsmittel und unterstützendes Werkzeug betrachtet wird, so sind in anderen Instituten Themen wie Netzsicherheit, angewandte Kryptographie, Hochverfügbarkeit, IT-Zuverlässigkeit und Vernetzung an sich integraler Forschungsgegenstand.
- Der Bedarf an Vertraulichkeit wird von vielen Faktoren beeinflusst. Neben den an jedem Institut vorhandenen unbedingt zu schützenden Informationen und Bereichen wie Verwaltungs- oder Personaldaten, gibt es oft auch vertrauliche Daten, Systeme oder sogar Netzwerke, die durch die Zusammenarbeit mit Projektpartnern entstehen, und ganz oder teilweise abgesichert werden müssen. Gerade bei Daten, die von außen durch einen ausgewählten Personenkreis zugreifbar sein müssen, tauchen weitere Probleme auf. Im Extremfall beinhaltet der zentrale Forschungsgegenstand eines ganzen Instituts bereits einen streng vertraulichen Themenbereich, so dass hier ein besonders hoher Anspruch an die Netzsicherheit und die Sicherheitspolitik als Ganzes besteht.
- Lokale Gegebenheiten haben einen nicht unbedeutenden Einfluss auf die Netzanbindung der verschiedenen Institute. Beispielsweise ergeben sich aus dem nahen Umfeld andere Randbedingungen. Mehr als die Hälfte der Standorte beherbergen lediglich eine einzige Entität; Daneben existieren aber auch Netzknoten in mehreren Städten, die bis zu zehn verschiedene Institute zusammenfassen und an das Internet anbinden. Teilweise befinden sich sogar mehrere Institute im selben Gebäude; Es finden sich aber auch Institute mit mehreren Gebäuden verteilt in einer Stadt oder sogar in ganz Deutschland. Auswirkungen zeigen auch die Nähe der Institute zu den lokalen Universitäten, die Größe der Niederlassungen und die Menge der übertragenen Daten. Je nach benötigter Bandbreite bestehen dabei unterschiedliche Anforderungen an die eingesetzte Hardware und die davon beeinflusste Netzwerkarchitektur.

Die bestehende Inhomogenität im Bereich der Anforderungen an die Netzanbindung und deren Sicherheit, Zuverlässigkeit und Vertraulichkeit hat zur Folge, dass das zentral erarbeitete Sicherheitskonzept respektive der zu dessen Umsetzung entwickelte Kommunikationsknoten nicht überall in unveränderter Form eingesetzt werden kann. Häufig müssen

kleinere, manchmal aber auch größere Änderungen oder Ergänzungen zum Kommunikationsknoten und zum Sicherheitskonzept durchgeführt werden. Die notwendigen Überarbeitungen der Vorgaben finden im Normalfall vor Ort in den Instituten statt. Dieser Prozess führt dazu, dass das Sicherheitsniveau gesellschaftsübergreifend nicht mehr zuverlässig vorhersagbar ist. Bei den dezentralen Änderungen am aufgestellten Sicherheitskonzept können bewusst oder unbewusst neue Sicherheitsschwächen hinzugefügt werden. Um nun zuverlässige Aussagen über das Sicherheitsniveau an den einzelnen Instituten treffen zu können und um die Einhaltung der vorgeschriebenen Sicherheitspolitik belegen zu können, sind Sicherheitsauditierungen unverzichtbar.

4 Überprüfung des Sicherheitsniveaus vor Ort

Wie in Kapitel 3 beschrieben, schafft die Heterogenität in der Umsetzung des IT-Sicherheitskonzepts bei den Fraunhofer Instituten und die daraus resultierende Notwendigkeit der lokalen Anpassung und Überarbeitung der vorgegebenen Sicherheitsregeln einen unverzichtbaren Bedarf an Auditierungen. Vor diesem Hintergrund hat die Fraunhofer Gesellschaft im Jahr 2002 eine stichprobenartige Sicherheitsauditierung von vier ausgewählten Instituten beauftragt. Die von uns durchgeführten Auditierungen fanden an vier von ihrer Umgebung und ihrer wissenschaftlichen Ausrichtung her möglichst unterschiedlichen Instituten statt. Die Sicherheitsuntersuchung beschränkte sich dabei auf die Kernkomponenten des vom Fh NOC entwickelten Kommunikationsknotens.

4.1 Vorgehensweise

In früheren Arbeiten wurde der Kommunikationsknoten bereits während der Entwicklung einer gründlichen Prüfung unterzogen. Grundlage hierfür waren Konzeptpapiere des Fraunhofer NOC und persönliche Gespräche mit den Entwicklern. Ziel dieser Arbeiten war zum einen das Aufdecken konzeptioneller Schwachstellen bereits zu Beginn der Entwicklung, zum anderen eine Bewertung des mit dem verfolgten Ansatz erreichbaren Sicherheitsgrades.

In einem zweiten Schritt wurden erste Vorabversionen des Kommunikationsknotens auf Konfigurationsschwachpunkte hin geprüft. Diese Untersuchung wurde sowohl manuell als auch unter Verwendung spezieller Prüfwerkzeuge vorgenommen. Gefundene Schwachstellen wurden dem Fraunhofer NOC mitgeteilt, um sie noch vor der Freigabe des Kommunikationsknotens für die Institute zu beseitigen. Dieser Schritt diente zum einen der ständigen Qualitätskontrolle, mit der die tatsächliche Implementierung bewertet werden sollte. Zum anderen wurde damit die Auditierung der einzelnen Institute im nächsten Schritt vorbereitet, indem die verwendeten Werkzeuge gemäß der gewünschten Sicherheitsparameter kalibriert wurden.

Im dritten Schritt, der in diesem Artikel detaillierter dargestellt wird, fand schließlich eine Untersuchung des Kommunikationsknotens im realen Betrieb statt. Hierfür wurden zunächst vier Fraunhofer Institute exemplarisch ausgewählt. Dabei wurde darauf geachtet, dass diese hinsichtlich der Anforderungen an die Netzanbindung ein möglichst breites Spektrum abdecken. Dieses reicht von der unveränderten Übernahme des NOC-Konzepts

über den Einsatz einer selbständig modifizierten und erweiterten Fassung bis hin zum Einsatz eines vollständig selbst entwickelten Konzepts.

Vor der eigentlichen Auditierung vor Ort in den Instituten wurde zunächst für jedes Institut der grundlegende Aufbau und die Struktur des lokalen Netzes ermittelt. Dies geschah auf Basis der Netzwerkdokumentation sowie der Konfigurationsdaten einiger essentieller Netzwerkkomponenten (vgl. Abschnitt 4.2), die von den IT-Verantwortlichen der einzelnen Institute zur Verfügung gestellt wurden. Diese Bestandsaufnahme ermöglichte einerseits eine Übersicht der spezifischen Anforderungen jedes Instituts an seine Netzanbindung, zum anderen wurden damit die Unterschiede der lokalen Konfigurationen zum generischen Kommunikationsknoten identifiziert und bewertet.

Bei den Untersuchungen vor Ort wurden diese Erkenntnisse und die Konsequenzen daraus dann mit den zuständigen IT-Verantwortlichen diskutiert, augenscheinliche Konfigurationsfehler dabei zum Teil direkt korrigiert. Ferner wurde der Wirkbetrieb der Kommunikationsknoten überprüft. Neben einer Untersuchung „von Hand“ wurden hierfür auch verschiedene Werkzeuge eingesetzt, die in Abschnitt 4.3 vorgestellt werden. Diese ermöglichen eine fundierte Untersuchung der eingesetzten Systeme auf Konfigurationsschwächen. In einer abschließenden Nachanalyse wurden alle Befunde nochmals in ihrer Gesamtheit bewertet und das Untersuchungsergebnis in einem Bericht zusammengefasst, der sowohl den Betreibern als auch den Entwicklern des Kommunikationsknotens übergeben wurde. Darüber hinaus wurden alle Einzelergebnisse miteinander korreliert. Damit sollten prinzipielle Schwachpunkte des Kommunikationsknotens aufgedeckt werden, die in zukünftigen Versionen zu beseitigen sind. Außerdem wurden so auch einige Probleme bezüglich der Handhabung aufgedeckt, die auf mögliche Ansatzpunkte für Verbesserungen bei der Schulung der IT-Techniker hinweisen.

4.2 Untersuchte sicherheitsrelevante Komponenten

Vor Ort wurden die Konfigurationen sämtlicher aus dem Internet angreifbarer Komponenten auf ihre Sicherheit hin überprüft. Hierzu zählen neben zentralen Unix-Systemen – z.B. Web- und FTP-Server – auch Netzkomponenten, wie etwa Firewall und Router. Diese Komponenten reichen in der Regel aus, um sämtliche Hauptdienste des Instituts zur Verfügung zu stellen. Die hier beschriebenen Erfahrungen mit der Auditierung beschränken sich daher auf die Betrachtung genau dieser Komponenten.

4.3 Verwendete Werkzeuge

Neben der immer notwendigen manuellen Analyse bei zu auditierenden Systemen kamen bei der Untersuchung auch mehrere Sicherheitswerkzeuge zum Einsatz. Gerade bei der zu erwartenden Ähnlichkeit der für die Netzanbindung sicherheitsrelevanten Komponenten stellen derartige Werkzeuge eine große Erleichterung dar. Dabei werden jeweils unterschiedliche Strategien verfolgt. Während es sich bei NESSUS [NES] um ein externes Penetrationswerkzeug handelt, fallen NIXE™ [GS02] und CROCODILE [GPS+03] in die Gruppe der Werkzeuge, die nach dem White-Box Verfahren arbeiten, also das jeweils zu untersuchende System von innen analysieren. Durch eine Prüfung der relevanten Systeme

von „innen heraus“ und von außen wird eine umfassende Sicht auf die Systeme ermöglicht, da somit sowohl Angriffe von Innentätern als auch solche externer Hacker simuliert werden.

4.3.1 NIXE™

NIXE™ (None-intrusive Unix Evaluation) [GS02] ist ein am Fraunhofer IESE entwickeltes Revisionswerkzeug für Unix-Plattformen, das nach dem White-Box Prinzip operiert. NIXE™ beschränkt sich ausdrücklich auf das Prüfen der zu untersuchenden Systeme. Es verzichtet bewusst darauf, den Konfigurationszustand zu verändern. Die detaillierte Bewertung der Prüfergebnisse und die Wahl geeigneter Reaktionen darauf bleiben dem Revisor vorbehalten, da vollautomatische Korrekturen leicht unerwünschte oder schwer absehbare Seiteneffekte haben können. Aufgrund seines neutralen Verhaltens kann das Werkzeug problemlos im laufenden Betrieb eingesetzt werden, ohne Sicherheit, Verfügbarkeit oder Integrität des Systems zu gefährden.

Um auf möglichst vielen verschiedenen Unix-Derivaten lauffähig zu sein, wurde für die Implementierung von NIXE™ auf den im Standardumfang jeder Unix-Konfiguration enthaltenen Bourne- bzw. Bash-Befehlsinterpreter zurückgegriffen, so dass das Werkzeug aus einem Satz von Shell-Skripten besteht. Zur Installation genügt es, diesen Satz von Skripten und Konfigurationsdateien im Textformat in ein beliebiges Verzeichnis des Zielsystems zu kopieren. Danach ist NIXE™ sofort startbereit und es bestimmt bei Bedarf zunächst die Installationspfade aller benötigten Systemkommandos automatisch. Im weiteren Verlauf wird dann ausschließlich auf diese Befehle zurückgegriffen, die auf allen gängigen Unix-Plattformen verfügbar sind. Auch bei der Wahl der verwendeten Befehlsparameter wurde auf größtmögliche Kompatibilität geachtet. Sämtliche Konfigurations- und Ergebnisdaten werden in separaten Unterverzeichnissen abgelegt. Somit lässt sich das Werkzeug rückstandslos entfernen, ohne Nebenwirkungen im Wirkbetrieb oder sonstige Spuren zu hinterlassen.

Die Prüflogik des Werkzeugs greift auf einen modularen Aufbau zurück, der es gestattet, nur die jeweils benötigten Prüfschritte durchzuführen. NIXE™ umfasst derzeit mehr als 20 Module, die unterschiedliche Sicherheitsaspekte des Zielsystems analysieren. Dabei liegt der Fokus beispielsweise auf einzelnen Diensten, auf systemweiten Konfigurationen, auf Benutzerkonten, auf Dateiberechtigungen oder sogar auf Hardware-Parametern. Zu den wichtigsten Prüfpunkten zählen:

- Überprüfung von Firmware- und Kernparametern,
- Untersuchung der Softwarekonfiguration bezüglich installierter Pakete und Patches,
- Analyse der vorhandenen Benutzerkonten hinsichtlich Passworteinstellungen, Gruppenzugehörigkeiten, Home-Verzeichnis, Suchpfad und konfiguriertem Befehlsinterpreter,
- Überprüfen auf Existenz bzw. Fehlen von Dateien und Verzeichnissen,
- Untersuchung von Dateien und Pfaden bezüglich der Attribute wie Eigentümer, Gruppenzugehörigkeit, Zugriffsrechte oder gegebenenfalls Prüfsumme,

- Analyse der Konfiguration der wichtigsten Dienste wie beispielsweise `atd`, `crond`, `ftpd`, `inetd`, `nfsd`, `sshd`, `syslogd` oder `telnetd`,
- Überprüfung der Protokollkonfiguration von `IP`, `TCP`, `UDP`, `SMTP` oder `SNMP` sowie eventuell damit verbundener Ports.

Die Prüftiefe der einzelnen Module lässt sich mittels Parametern zur Laufzeit variieren. Dies hat Einfluss auf die Dauer des Analyselaufes und vor allem auf den Umfang des generierten Prüfprotokolls.

Nach Beendigung des Analyselaufes werden die ermittelten Ergebnisse in fünf Gefahrenstufen klassifiziert ausgegeben (siehe Tabelle 1). Die Prüfergebnisse sind nach Gefahrenstufen getrennt voneinander darstellbar, was eine schnelle Übersicht über die besonders kritischen Befunde ermöglicht.

Klasse	Erläuterung
OKAY	sinnvolles Merkmal
INFO	neutrales Merkmal
CHECK	unklare Gefahrenlage
WARN	potentieller Mangel
ALERT	gravierender Mangel

Tabelle 1: Die Gefahrenstufen von NIXE™

Um eine zeitraubende und fehlerträchtige manuelle Eingabe sämtlicher Prüfvorgaben zu vermeiden, generiert NIXE™ abhängig vom Prüfgegenstand automatisch eine Initialversion der Prüfregeln. Die Idee besteht darin, die Werkzeugkonfiguration von einem Referenzsystem abzuleiten, das den jeweils zu prüfenden Systemen möglichst gut entspricht. NIXE™ extrahiert in einem Konfigurationslauf die relevanten Sicherheitsmerkmale des Referenzsystems und bildet daraus entsprechende Prüfvorgaben. Als Referenzsystem kann willkürlich eines der zu untersuchenden Systeme ausgewählt werden; es bedarf keiner separaten Installation. Je präziser jedoch das verwendete Referenzsystem konfiguriert ist, desto schärfer sind die damit erzielten Befunde. Es lassen sich zusätzlich eigene Prüfvorgaben ergänzen, etwa solche, die das System nicht automatisch ableiten konnte oder die über den Standardumfang von NIXE™ hinaus gehen. Die Funktionsweise von NIXE™ ist in Abbildung 1 nochmals im Überblick dargestellt.

Der Benutzer hat die Möglichkeit, je nach Anwendungsfall und Umfang des Revisionsvorhabens den Vorbereitungsaufwand gegen die Analyseschärfe abzuwägen, um letztlich auch die Gesamtkosten der Revisionskampagne zu minimieren. Für ein einzelnes zu untersuchendes System bietet es sich beispielsweise an, einfach eine der Standardvorgaben als Referenz zur Analyse zu verwenden. In diesem Fall erhält man ein etwas unschärferes Prüfresultat zugunsten einer schnellen und bequemen Einsatzfähigkeit. Sollen mehrere gleiche oder gleichartige Systeme untersucht werden, rechnet sich der investierte Aufwand für das Erstellen eines möglichst sicher konfigurierten Referenzsystems bzw. für die sorgfältige Feinjustage der Konfiguration. Dadurch fallen die erzielten Ergebnisse der eigentlichen Prüfläufe deutlich kompakter und schärfer aus.

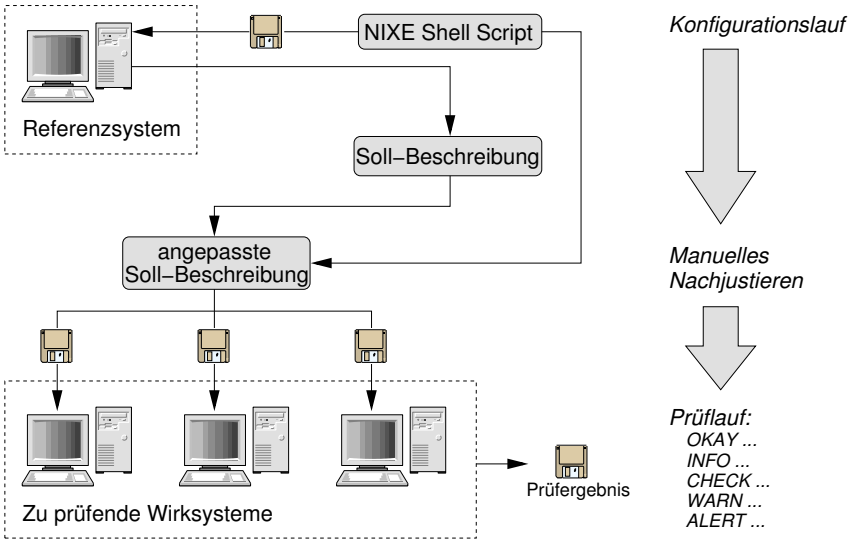

Abbildung 1: Funktionsweise von NIXE™ im Überblick

4.3.2 CROCODILE

Das ebenfalls am Fraunhofer IESE entwickelte CROCODILE (Cisco Router Configuration Diligent Evaluator) [GPS+03] ist ein Auditierungswerkzeug zur Analyse von Router-Konfigurationen. Auch bei CROCODILE handelt es sich um ein flexibles, modular aufgebautes Werkzeug. Im Mittelpunkt steht ein Parser, der die zu analysierenden textuellen Konfigurationsdateien nach bestimmten Mustern durchsucht. Jedes Modul liefert dabei dem Parser eine Liste ihm bekannter Suchmustern, für die es eine Bewertung abgeben kann. Jedesmal, wenn der Parser beim Abarbeiten einer Konfigurationsdatei auf eines dieser Muster trifft, werden die zugehörigen Module benachrichtigt und so die passenden Behandlungsroutinen initiiert. CROCODILE unterstützt sehr einfache Suchmuster und Behandlungsroutinen. Dennoch gehen die Möglichkeiten des Werkzeugs bei weitem über das Prüfen auf Existenz oder Nicht-Existenz von einzelnen Konfigurationsanweisungen hinaus. CROCODILE ist in der Lage, mehrere Konfigurationsanweisungen dateiübergreifend in Zusammenhang zu bringen und kontextuell zu bewerten.

CROCODILE stellt verschiedene Module zur Verfügung, die unterschiedlichste Prüfbereiche abdecken. In Tabelle 2 sind einige der wichtigsten Prüfmodule aufgeführt.

Die meisten Module können völlig unabhängig voneinander in das Prüfwerkzeug „eingebettet“ werden. Einige Module tauschen jedoch Analysedaten und Ergebnisse untereinander aus. Ein Beispiel hierfür ist das Connectivity-Modul, das grundlegende Informationen an verschiedene andere Module weiterreicht.

Eine weitere Besonderheit von CROCODILE findet sich in der Analyse und Bewertung der Zugangskontrolllisten (ACLs) eines Routers. Selbst Netzwerkspezialisten können oft nur schwerlich die Integrität, Konsistenz und Sicherheit aller ACLs gewährleisten. Hier

Modul	Beschreibung
IngressEgress	Mit diesem Modul lassen sich fundamentale IP-Filter Eigenschaften von Router-Schnittstellen oder Zugriffskontrolllisten (ACLs) verifizieren. Es können beliebige benutzerdefinierte Blacksets und Whitesets angegeben werden, gegen die die Konfigurationsdateien geprüft werden, beispielsweise Anti-Spoofing Regeln [FS00, RMK+96] für Perimeter-Router.
SNMP	Dieses Modul überprüft die Einstellungen des Simple Network Management Protocols, um die Gefahr eines nicht autorisierten Administrationszugangs auf den Router zu verringern.
NTP	In diesem Modul werden widersprüchliche Konfigurationseinstellungen des Network Time Protocols aufgespürt. Zusätzlich wird eine Aufstellung aller für das NTP relevanten Netzwerkgeräte (Clients und Server) generiert.
AAA	Dieses Modul beschäftigt sich mit dem Themenkomplex Authentifizierung, Autorisierung und Abrechnung, wobei sich die vorliegende Version auf das Prüfen der Integrität, Konsistenz und Sicherheit der lokalen und servergestützten Authentifizierung konzentriert (Radius oder Tacacs+).
SingleClauses	Hierbei handelt es sich um ein generisches Prüfmodul mit frei konfigurierbaren Evaluationskriterien. Angaben können in einem einfachen und gleichzeitig flexiblen Format gemacht werden.

Tabelle 2: Ausgewählte CROCODILE Module

hilft das Werkzeug mit seinen Fähigkeiten, nicht nur Aussagen über das Weiterleiten von einzelnen Paketen treffen zu können. CROCODILE ist darüber hinaus auch in der Lage, die vollständigen Mengen aller weiterzuleitenden und aller zu verwerfenden Pakete für alle Schnittstellen separat zu berechnen. Dies ermöglicht es, auf einfache Weise zu überprüfen, ob eine benutzerdefinierte Vorgabe von Blacklists und Whitelists vom Router eingehalten wird. Zusätzlich werden bei dieser Berechnung automatisch sogenannte „tote Regeln“ aufgespürt. Darunter werden Regeln zur Paketfilterung verstanden, die vollständig von vorangegangenen Filterregeln abgedeckt werden und die somit nicht zum Tragen kommen. Sie sollten aus Gründen der Konsistenz und zur Verbesserung der Router-Performance aus der Konfiguration entfernt werden.

Eine weitere Unterstützung bietet CROCODILE dem Auditor durch eine Aufzählung aller in der Router-Konfiguration erwähnten Subnetze und Netzwerkknoten sowie derjenigen Schnittstellen, über die diese erreichbar sind. Dieser Überblick ermöglicht eine schnelle Abschätzung der Netzwerkstruktur.

Nach erfolgreichem Analyselauf erzeugt CROCODILE eine Ergebnisdatei im XML-Format, aus dem sich prinzipiell Ergebnisdarstellungen beliebiger Formate generieren lassen. Zusätzlich wird eine interaktive Ergebnisdarstellung im HTML-Format erzeugt (vgl. Abbildung 2). Hier lassen sich die Resultate nach Kontexten sortiert betrachten. Die Ergebnisse werden wiederum in den fünf bereits bekannten Gefahrenstufen (siehe Tabelle 1) dargestellt. Einen schnellen Überblick liefert ein farbiges Balkendiagramm, das die Ergebnisse der einzelnen Module symbolisch wiedergibt. Durch die Interaktivität lässt sich aus dieser Gesamtübersicht bis hinunter in Detailangaben zu einzelnen Prüfpunkten

navigieren. Zur Erleichterung der Analyse werden zu den auftretenden Router-Befehlen Verknüpfungen auf die jeweilige Online-Dokumentation geliefert.

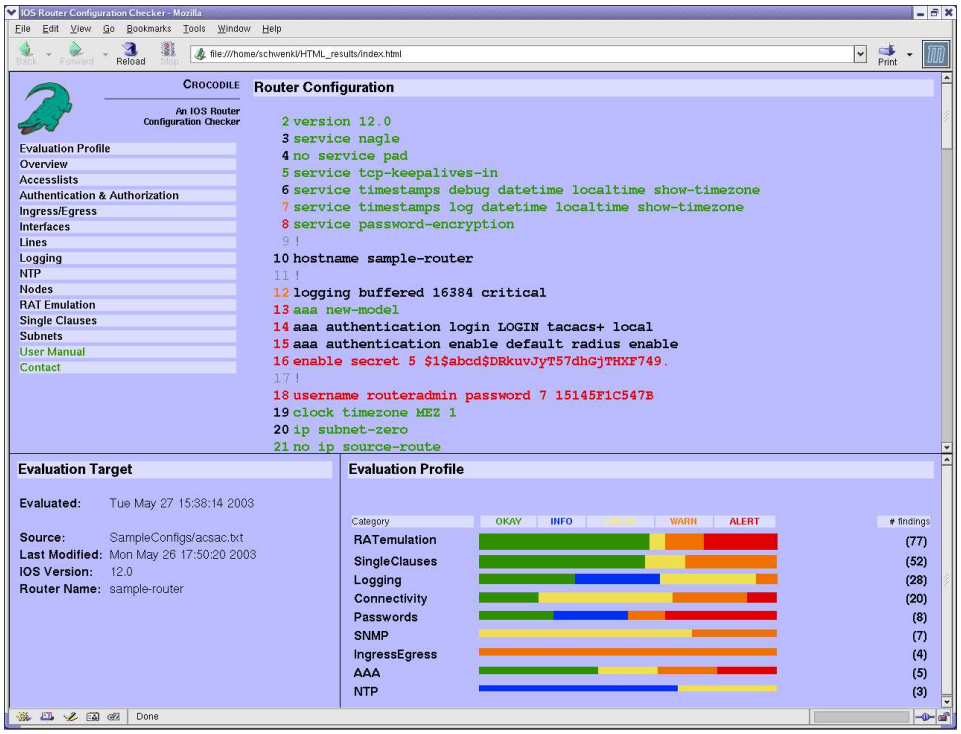

Abbildung 2: Interaktive Ergebnisdarstellung von CROCODILE im HTML-Format

4.3.3 NESSUS

Das dritte verwendete Auditierungswerkzeug unterscheidet sich von den vorangegangenen durch seinen grundlegend anderen Analyseansatz. NESSUS [NES] überprüft eine Vielzahl von Netzwerkkomponenten nach dem Black-Box Ansatz. Dafür analysiert es ein Netzwerk von außen und stellt somit eine ideale Ergänzung zu den beiden nach dem White-Box Verfahren operierenden Analysewerkzeugen NIXE™ und CROCODILE dar.

NESSUS ist ein von Renaud Deraison und anderen entwickeltes, frei verfügbares Penetrationswerkzeug, das auf Client-Server Basis fungiert. Der Server repräsentiert dabei das agierende System, während ein oder mehrere Clients die Visualisierung der Konfiguration und der Ergebnisse übernehmen. Dabei ist der Server in der Lage, eine praktisch unbegrenzte Anzahl von Zielsystemen parallel zu überprüfen.

Das Werkzeug ist modular aufgebaut. Jeder einzelne Prüfpunkt wurde als unabhängiges Modul implementiert. Zur Optimierung des Analyselaufs ist NESSUS in der Lage, nur

wirklich benötigte oder sinnvolle Module in die Auditierung einzubeziehen. Die Entwicklung von neuen Modulen wird durch die Nessus Attack Scripting Language (NASL) deutlich vereinfacht. Auf diese Art kann binnen kürzester Zeit auf neue Sicherheitslücken reagiert und das Werkzeug um entsprechende Prüfpunkte erweitert werden. Zur Zeit existieren mehr als 1500 Module, die eine Vielzahl verschiedenster Analyseschritte beinhalten. Die zentrale Datenbank der verfügbaren Prüfmodule wird täglich aktualisiert.

Zur Erhöhung der Interoperabilität mit anderen Herstellern ist die Befundausgabe von NESSUS kompatibel zum Common Vulnerabilities and Exposures (CVE) Standard [Mar01]. So können entdeckte Schwachstellen eindeutig identifiziert und mit den zugehörigen Korrekturmaßnahmen in Beziehung gesetzt werden.

In den Prüfgegenständen spiegelt sich der Black-Box Ansatz derart wider, dass das Werkzeug keinerlei Voraussetzungen an seine Umgebung stellt. Unabhängig von der durch die Internet Assigned Numbers Authority (IANA) festgelegten Port-Nummern-Zuweisungen findet NESSUS autark die sichtbaren Dienste und identifiziert die damit verbundenen Programme und Versionen. Module zur Suche nach vorhandenen Sicherheitsschwachstellen werden jedoch nur auf korrekt identifizierte Systeme angewendet. Diese aggressive Verfahrensweise, die zum Absturz des überprüften Systems führen kann, lässt sich bei Bedarf deaktivieren, um den Betrieb einer Produktivumgebung nicht unnötig zu gefährden.

Schließlich kann NESSUS auch mit anderen Sicherheitswerkzeugen kombiniert werden um so den Analyseumfang auszuweiten. Tabelle 3 führt einige der unterstützten Werkzeuge auf und beschreibt die dadurch erzielbaren Erweiterungen des Prüfumfangs.

Werkzeug	**Erweiterung des Prüfumfangs**
NMAP [NMA]	Erweitert die Möglichkeiten für eine Port-Abtastung.
NIKTO [NIK] und WHISKER [WHI]	Stellen weiterführende Prüfmöglichkeiten für Web-Server und CGI-Programme bereit.
HYDRA [HYD]	Ergänzt den Analyseumfang um die Möglichkeit eines Brute-Force-Angriffs auf verschiedene herkömmliche Dienste.

Tabelle 3: Software zur Erweiterung des Prüfumfangs von NESSUS

Die durch einen Prüflauf erzielten Ergebnisse werden von NESSUS im werkzeugeigenen Fenster dargestellt (siehe Abbildung 3). Auf Wunsch können die Ergebnisse auch in den Datenformaten XML, HTML, ASCII oder LaTeX exportiert werden. Dabei unterscheidet das Werkzeug zwischen drei verschiedenen Klassifikationen (Kommentar, Warnung, Sicherheitslücke), die wiederum in sechs Risikostufen unterteilt sind (vergleiche hierzu die Tabellen 4 und 5).

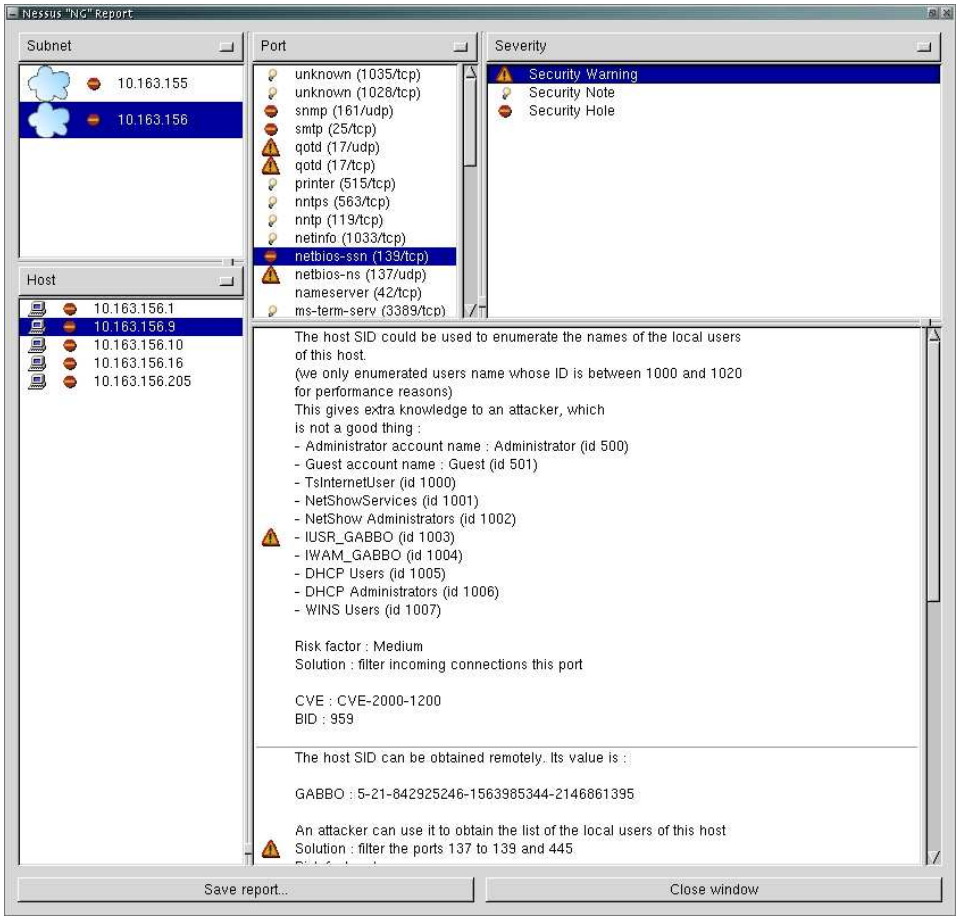

Abbildung 3: Ergebnisausgabe von NESSUS

5 Untersuchungsergebnisse

Im Rahmen dieses Artikels kann natürlich nicht konkret auf vorgefundene Schwachpunkte eingegangen werden. Trotzdem können einige allgemeine Aussagen über das Untersuchungsergebnis und die bei der Auditierung gewonnenen Erfahrungen gemacht werden, ohne dabei die IT-Sicherheit innerhalb der FhG zu gefährden.

Zunächst ist festzuhalten, dass das beschriebene Vorgehen bei Instituten, die den Kommunikationsknoten durch ein eigenes Konzept ersetzt haben, nur bedingt greift. Hier muss eine erneute vollständige Auditierung durchgeführt werden, d.h. alle drei in Kapitel 4.1 beschriebenen Schritte müssen erneut durchlaufen werden.

Ansonsten ergab die Auditierungskampagne ein insgesamt positives Bild. So konnte die Sicherheit aller untersuchten Institute deutlich verbessert werden, selbst wenn die zuständigen IT-Verantwortlichen nur über rudimentäre IT-Sicherheitskenntnisse verfügten. Die

Klasse	Erläuterung
Security note	Liefert einen unkritischen Kommentar.
Security warning	Warnt vor einem möglichen Sicherheitsproblem.
Security hole	Meldet einen gravierenden Sicherheitsmangel.

Tabelle 4: Klassifikation von Analyseergebnissen bei NESSUS

Klasse	Erläuterung
NONE	Keine inhärenten Risiken.
LOW	Das Prüfergebnis stellt keine Bedrohung an sich dar, das berichtete Problem kann einem Angreifer aber eventuell hilfreiche Informationen liefern.
MEDIUM	In Zusammenhang mit anderen Sicherheitslücken kann das gemeldete Problem ein schwerwiegendes Sicherheitsloch öffnen.
HIGH	Gefahr eines unerwünschten Zugriffs.
SERIOUS	Ein Sicherheitsloch besteht, durch das ein Angreifer wertvolle Informationen erhalten kann.
CRITICAL	Das System konnte kompromittiert werden.

Tabelle 5: Risikoeinstufung der Analyseergebnisse bei NESSUS

gewählte Firewall-Architektur erwies sich als gute Basis für die meisten gängigen Standardfälle. Sie ermöglicht problemlos einfachere Anpassungen an örtliche Gegebenheiten, wie sie von einigen Administratoren durchgeführt wurden. Dabei wurde sichtlich versucht, sich an den Vorgaben des NOC zu orientieren und eigene Modifikationen sorgfältig zu dokumentieren. Der Kommunikationsknoten eignet sich damit für die Internet-Anbindung von Instituten mit normalen bis durchschnittlichen Funktionsanforderungen.

Die verbliebenen Schwachstellen lassen sich größtenteils dem Bereich organisatorischer Maßnahmen zurechnen. Neben der Verwendung bekannter Standardzugangspasswörter sind hier vor allem Fehlern in der verwendeten Software zu nennen. So konnten mehrere Schwachstellen in Systemprogrammen nachgewiesen werden, für deren Behebung bereits Patches zur Verfügung stehen. Teilweise wurde auf diesen Umstand schon bei der konzeptuellen Überprüfung vor Freigabe des Kommunikationsknotens hingewiesen. An einigen Standorten war die physische Absicherung der Netzkomponenten nicht ausreichend. Auch die Verwendung unsicherer Programme wie z.B. Telnet anstelle wesentlich sicherer Alternativen wie SSH muss moniert werden. Auffällig war auch, dass mit steigendem Know-How des zuständigen Personals statt der zum Kommunikationsknoten gehörenden graphischen Administrationsoberfläche lieber auf altbewährte Konfigurationswerkzeuge zurückgegriffen wurde, typischerweise eine einfache Shell.

6 Zusammenfassung und Ausblick

Wir haben im vorliegenden Artikel erste Erfahrungen mit dem Kommunikationsknoten der Fraunhofer Gesellschaft im Praxiseinsatz beschrieben. Grundlage unserer Betrachtun-

gen war eine Auditierungskampagne bei ausgewählten Fraunhofer Instituten kurz nach Installation der neuen Netzanbindung.

Die FhG ist mit der Einführung des Kommunikationsknotens ihrem Ziel, einen gesellschaftsweiten Mindeststandard für die Sicherheit der Internet-Konnektivität und der Kommunikation der Institute untereinander aufzubauen, einen entscheidenden Schritt näher gekommen. So wird durch das generische Konzept und dessen Implementierung in Form des Kommunikationsknotens allen Instituten eine sichere Netzanbindung ermöglicht, auch wenn diese über kein für IT-Sicherheitsfragen besonders qualifiziertes Personal verfügen. Für die örtlichen IT-Verantwortlichen stellt der Knoten darüber hinaus eine gute Diskussionsgrundlage dar, um mit der Institutsleitung notwendige Investitionen zu planen.

Trotz allem ist während der Untersuchungen aber auch deutlich geworden, dass die Bereitstellung von technischen Mitteln alleine nicht ausreicht, sondern IT-Sicherheit als andauernder Prozess aufgefasst werden muss. Im folgenden werden die in unseren Augen wichtigsten Punkte zusammengefasst, um den Kommunikationsknoten weiter zu verbessern und so die Gesamtsicherheit zu steigern:

- *Sichere Software-Versionen und -Konfigurationen*
  Die Ausnutzung bekannter Sicherheitsschwächen in Software und deren Konfigurationen dürfte der häufigste Angriff auf Systeme im Internet sein. Deshalb sollte strikt darauf geachtet werden, möglichst aktuelle Programmversionen einzusetzen. Bei der Untersuchung vor Ort musste allerdings festgestellt werden, dass zum Teil alte und anfällige Software zum Standardumfang des Kommunikationsknotens gehört. Ähnliches gilt für unsichere Konfigurationseinstellungen. Diese Lücken wurden teilweise durch die örtlichen Administratoren behoben. Da hierzu jedoch detaillierte Kenntnisse nötig sind, sollte dies besser zentral durch das NOC erfolgen. Dieses hat zwar mittlerweile den Kommunikationsknoten um einen grundlegenden Wartungsservice erweitert, mit dessen Hilfe die einzelnen Institute auf Knopfdruck aktuelle Patches einspielen können. Selbst vorgenommene Konfigurationsänderungen können dadurch jedoch verloren gehen. Diese nach jedem Update erneut einzuarbeiten ist ein zu fehleranfälliger Prozess. Hier muss gemeinsam nach geeigneten Lösungen gesucht werden, die insbesondere auch diejenigen Administratoren berücksichtigen müssen, die nicht die mitgelieferte Wartungssoftware einsetzen.
- *Organisatorische Sicherheit*
  Vereinzelt konnten organisatorische Sicherheitsmängel festgestellt werden. So waren manche Komponenten beispielsweise nicht hinreichend vor unbefugten physischen Zugriffen geschützt. Alle Beteiligten müssen sich bewusst machen, dass die zentral bereitgestellte Technik für eine sichere IT-Infrastruktur nicht ausreicht. Insbesondere kann sie eine ausreichende Qualifizierung der örtlichen IT-Verantwortlichen nicht vollständig ersetzen. Die bereits ergriffenen Schulungsmaßnahmen sollten deshalb ausgeweitet werden. Besonderes Augenmerk verdient dabei die Rolle des örtlichen IT-Personals als Multiplikator für die anderen Mitarbeiter eines Instituts. Nur wenn die Sicherheitspolitik von *allen* Mitarbeitern in der FhG gelebt wird, kann sie auch erfolgreich sein.
- *Erweiterung des Anforderungsprofils*
  Der modulare Aufbau des Kommunikationsknotens sollte weiter vorangetrieben wer-

den, um mit den ständig wachsenden Anforderungen in der Praxis mithalten zu können. Parallel dazu ist das Sicherheitskonzept weiterzuentwickeln. Schon heute stößt man an Grenzen, wenn Institutsaußenstellen angebunden oder gesonderte Netzbereiche für die Zusammenarbeit mit externen Projektpartnern realisiert werden sollen. Diese benötigen typischerweise Zugriff auf Teile des Intranets. Interne Kalkulationsdaten aber sollte ein externer Projektpartner nicht einsehen dürfen. Zur Realisierung solcher Szenarien bedarf es aufwendiger Änderungen am Kommunikationsknoten. So erfordert die Anbindung einer Vielzahl einzelner externer Arbeitsplätze über ein Virtual Private Network (VPN) die Einbettung einer fraunhoferweiten Public Key Infrastructure (PKI). Die laufenden Arbeiten der Fraunhofer Zentrale für den Aufbau einer solchen Infrastruktur sollten in zukünftige Versionen des Kommunikationsknotens einfließen. Weitere drängende Probleme sind die Behandlung von Festangestellten im Vergleich zu Teilzeit- bzw. studentischen Hilfskräfte oder institutsfremden Mitarbeitern und sonstigen Gästen sowie die von im Institutsgebäude angesiedelten Spin-Offs. Derzeit existieren im Intranet keine abgestuften Sicherheitszonen, d.h. jeder Mitarbeiter hat vollen Zugang zum gesamten Intranet. Ausgenommen hiervon sind lediglich personenbezogene und Verwaltungsdaten. Jeder Mitarbeiter genießt also volles Vertrauen; selbst wenn man niemandem böswillige Absicht unterstellt, so zeigt die Praxis doch, dass dies nicht gerechtfertigt ist [MS02]. Neben diesen organisatorischen Aspekten wachsen auch die Wünsche der Nutzer und damit die technischen Anforderungen an den Kommunikationsknoten. Neben Wireless LANs seien hier beispielsweise die immer häufiger auftretenden Applikationsserver auf Java-Basis genannt. Diese bieten Dienste im Internet an, delegieren Teilaufgaben aber meist an Systeme im Intranet. In vielen Instituten sind solche Situationen bereits heute Alltag. Dies führte zu einer Vielzahl individueller Lösungen, die nur zum Teil mit dem zentralen Konzept abgestimmt sind. Schon aus wirtschaftlichen Gründen sollten diese Arbeiten zumindest zentral koordiniert werden. Dies sollte auch im Interesse der Institute sein, die so eine Bestätigung für die Sicherheit und Qualität ihres Entwurfs erhalten.

- *Neue Sicherheitstechniken*
  Auch wenn Sicherheit heute primär als Prozess begriffen wird, so benötigt man doch verschiedene Techniken um die Komplexität aktueller Systeme handhabbar zu machen. Hierzu gehören beispielsweise Mechanismen zur Abwehr von Spam-Mails, Werkzeuge zur systematischen Analyse von Log-Daten sowie Intrusion Detection Systeme (IDS), mit deren Hilfe Angriffe auf ein System aufgedeckt werden können. Der Kommunikationsknoten wird gerade auch in diesen Bereichen aktiv weiterentwickelt. Dieser Weg sollte weiter beschritten werden, insbesondere die Log-Datenanalyse hat ein großes Potential sowohl die Sicherheit als auch die Robustheit des Systems zu verbessern. Eine entsprechende Werkzeugunterstützung in diesem Bereich kann auch als Einstieg in ein IDS angesehen werden. Nahe liegend ist auch die Integration von Auditwerkzeugen in den Standardumfang des Kommunikationsknotens, so dass der örtliche IT-Verantwortliche in regelmäßigen Abständen selbständige Audits durchführen kann.

Die vorgestellten Ergebnisse können prinzipiell auf andere Umgebungen übertragen werden. Denkbar sind zum Beispiel Universitätsrechenzentren, die mit der Netzanbindung von Fakultäten und Lehrstühlen vor ähnliche Herausforderungen gestellt werden. Aber

auch mittelständische und große Unternehmen sehen sich mit denselben Problemen konfrontiert. Der Kommunikationsknoten bietet hier eine gute Ausgangsbasis. Das Fraunhofer NOC hat dies erkannt und bemüht sich, den Kommunikationsknoten auch außerhalb der Fraunhofer Gesellschaft zu vermarkten [NOC]. Mit steigender Verbreitung des Kommunikationsknotens wird sich nach unserer Überzeugung zukünftig vor allem der Erfahrungsaustausch zwischen Entwicklern und Betreibern aber auch zwischen den Betreibern untereinander als wesentliche Herausforderung herauskristallisieren. Diese gilt es zu bewältigen. Damit ließe sich auch das erhebliche Potential des in der Fraunhofer Gesellschaft verteilt vorhandenen Wissens für alle nutzbar machen. Möglichkeiten hierfür bieten Techniken, wie sie im Erfahrungsmanagement angewendet werden. Dazu gehören beispielsweise Case-based Reasoning, wissensbasierte Datenbanken und über das Netzwerk zugreifbare moderierte Diskussionsforen. Ein erstes Beispiel für die Anwendung dieser Techniken zur Verbesserung der IT-Sicherheit wird in [NGS03] beschrieben. Auch die teilweise Auslagerung der Auditierung an die lokalen Systemadministratoren bzw. IT-Sicherheitsverantwortlichen im Sinne einer Qualitätssicherung ist durch geschickten Einsatz von intelligenten Werkzeugen möglich und kann zur Steigerung des Gesamtsicherheitsniveaus positiv beitragen.

Danksagung

Wir möchten uns an dieser Stelle bei der Fraunhofer Zentralverwaltung sowie den Mitarbeitern des Fraunhofer NOC in Karlsruhe für die gute Zusammenarbeit bedanken. Stellvertretend seien hier Herr Peter Kiesel und Frau Heike Schwingel-Horner genannt. Ein herzliches Dankeschön auch den IT-Verantwortlichen der überprüften Institute für ihre Kooperation.

Literatur

[FS00] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing (RFC2827). ftp://ftp.rfc-editor.org/in-notes/rfc2827.txt, May 2000.

[GPS+03] Stephan Groß, Holger Peine, Thomas Schwenkler, Reinhard Schwarz, and Kai Simon. CROCODILE *Benutzerhandbuch – Der Cisco Router Configuration Diligent Evaluator*. Fraunhofer IESE, Kaiserslautern, 2.1 edition, January 2003. IESE Report-Nr. 067.02/D.

[GS02] Stephan Groß and Reinhard Schwarz. NIXE – *Ein Werkzeug für Unix Sicherheitsrevisionen. Anwenderhandbuch*. Fraunhofer IESE, Kaiserslautern, 1.0 edition, February 2002.

[HON02] Wolke Neun kaputt gehackt. Heise Online News, February 2002. http://www.heise.de/newsticker/data/gr-02.02.02-004/.

[HYD] THC Hydra. http://www.thc.org.

[Mar01] Robert A. Martin. Managing Vulnerabilities in Networked Systems. *IEEE Computer Society*, 34(11):32–38, November 2001.

[McH01] John McHugh. Intrusion and Intrusion Detection. *International Jounal of Information Security*, 1(1):14–35, 2001.

[MS02] Kevin D. Mitnick and William L. Simon. *The Art of Deception. Controlling the Human Element of Security*. John Wiley, Chichester, October 2002.

[NES] The Nessus Project. http://www.nessus.org/.

[NGS03] Markus Nick, Stephan Groß, and Björn Snoek. How Knowledge Management Can Support the IT Security of eGovernment Services. In M.A. Wimmer, editor, *Knowledge Management in Electronic Government. 4th IFIP International Working Conference, KMGov 2003. Proceedings*, number 2645 in LNAI, pages 151–162, Rhodes, Greece, May 2003. Springer Verlag.

[NIK] Nikto. http://www.cirt.net/code/nikto.shtml.

[NMA] Network Mapper. http://www.insecure.org/nmap.

[NOC] Fraunhofer NOC. Sicherer Kommunikationsknoten. Produktprospekt, Fraunhofer IITB, http://www.iitb.fhg.de/servlet/is/4414/.

[RMK+96] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address Allocation for Private Internets (RFC1918). ftp://ftp.rfc-editor.org/in-notes/rfc1918.txt, February 1996.

[Sch00] Bruce Schneier. *Secret and Lies. Digital Security in a Networked World.* John Wiley, Chichester, 2000.

[WHI] Whisker. http://www.wiretrip.net/rfp/p/doc.asp/i2/d21.htm.