Kommunikationslage im Blick

Gefahr erkannt, Gefahr gebannt

Die IT-Sicherheitsereignisse der jüngsten Vergangenheit haben weitreichende Auswirkungen – sowohl für Menschen als auch für Unternehmen: 50 Milliarden Euro Schaden im Jahr im Bereich Wirtschaftsspionage allein in Deutschland, so die Aussagen des Bundesinnenministeriums. Der große Lauschangriff auf Politik, Industrie und Wirtschaft ist Realität und hat wesentlich größere Ausmaße, als die ohnehin schon pessimistischen Experten in der Vergangenheit vermutet hatten. Jeden Tag steigt die Anzahl an erfolgreichen Angriffen, sowohl im Bereich Software (Heartbleed, Windows XP, Schwachstellen in Browsern, Betriebssystemen und Anwendungen ...) als auch im Bereich von Hardware (datensammelnde Smart-TVs, Lücken in Routern, ausspähende Bügeleisen und Computermäuse …). Ohnmacht macht sich vielerorts breit. Dennoch gibt es Strategien, die helfen, die Risiken nachhaltig zu reduzieren. Die Herausforderung ist dabei, eine sehr gute Sichtweise über die gesamte Kommunikationslage zu erlangen, Wissen über die eigene Kommunikation und die verwendeten Technologien aufzubauen und zu nutzen, aus der Vergangenheit zu lernen sowie mit anderen zusammenzuarbeiten, um aus den Erkenntnissen angemessene Gegenmaßnahmen einzuleiten.

Die größte Gefahr besteht immer dann, wenn Bedrohungen falsch eingeschätzt werden. Wer die Gefahren hingegen kennt, kann sich und seine Werte besser schützen. Mithilfe eines Kommunikationslagebildes sollen Angriffe auf die IT-Systeme und Werte (also die Daten) einer Organisation erkannt sowie die Schwachstellen der benutzten Technologien und Internet-Protokolle aufgezeigt werden. So lässt sich ein wirkungsvolles und nachhaltiges Schutzkonzept entwickeln. Dies wird mit den drei wichtigsten Kernaspekten ermöglicht:

1. Angriffe und Schwachstellen müssen zuerst identifiziert werden.
2. Die daraus resultierenden Gefahren müssen bewertet werden.
3. Nach Identifikation und Bewertung können Risiken gezielt angegangen und auf ein angemessenes Maß minimiert werden.

Generierung eines Kommunikationslagebildes

Beispielsweise lässt sich ein vollständiges Kommunikationslagebild mithilfe des vom Institut für Internet-Sicherheit – if(is) entwickelten Internet-Analyse-Systems (IAS) ermitteln. Dabei wird ein spezieller IAS-Sensor meist zwischen dem Unternehmensnetzwerk und dem Internet positioniert. Der Sensor ist in der Lage, bis zu 3.000.000 potenzielle Kommunikationsmerkmale in den Kommunikationspaketen zu identifizieren und dann zu zählen. Das funktioniert analog zu einer Strichliste: Wird das Kommunikationsmerkmal erkannt, wird es gezählt. Ein Kommunikationsmerkmal kann ein Kommunikationspa-

rameter oder eine Verknüpfung von verschiedenen Kommunikationsparametern sein. In Abbildung 1 sind exemplarisch IPv6, IPv4, TCP, UDP, HTTP, HTTPS und SMTP, sieben der 3.000.000 möglichen Kommunikationsmerkmale dargestellt (1).

Mit diesem Prinzip werden die sicherheitsrelevanten Informationen aus dem Datenstrom extrahiert. Wichtig ist, dass so viele sicherheitsrelevante Informationen wie möglich festgehalten werden. Außerdem ist es wichtig, dass der Reduzierungsgrad der Bytes der eigentlichen Kommunikationsdaten und der sicherheitsrelevanten Informationen sehr groß ist, um diese langfristig nutzen zu können. Beim IAS hat sich herausgestellt, dass eine Zählzeit der Strichliste von fünf Minuten ideale Werte erbringt. Bei einer typischen IAS-Sonde werden so circa zehn GByte Daten pro Jahr gesammelt. Das Prinzip der Ermittlung von Kommunikationsmerkmalen ist dabei datenschutzkonform. Das heißt, es werden keine Nutzerdaten, IP-Adressen oder sonstige personenbezogene oder -beziehbare Informationen bewertet (Quelle: /PePo11/).

Die Kommunikationsmerkmale zeigen dabei sicherheitsrelevante Informationen über verschiedene Aspekte wie Angriffe (Ports, SYS-ACK etc.), genutzte Technologien (User-Agent, Versionen von Technologien und Standards etc.) und die Nutzung/Verteilung von Protokollen und Anwendungen an. Dadurch erlauben sie es, die Kommunikationslage ermitteln, darstellen und bewerten zu können. Erst durch diese Maßnahme wird wirklich zu jedem Zeitpunkt live und nachhaltig sichtbar, was im eigenen Netzwerk eigentlich passiert und welche Technologien und Protokolle daran beteiligt sind.

Das Kommunikationslagebild zeigt nicht nur die IT-Sicherheitsprobleme, sondern die Gesamtlage, also auch den Anteil sicherer Eigenschaften des Systems (Netzwerkes). Aus diesem Grund kann das Kommunikationslagebild auch als Darstellung des Gesundheitszustandes des eigenen Netzwerkes und der daran angeschlossenen IT-Systeme betrachtet werden.

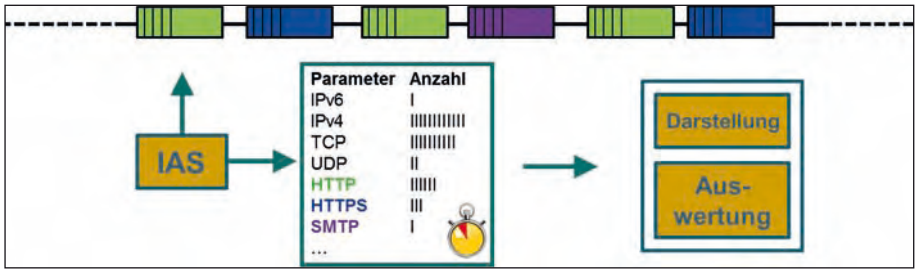


Abb. 1.: Prinzip der Extrahierung der sicherheitsrelevanten Informationen

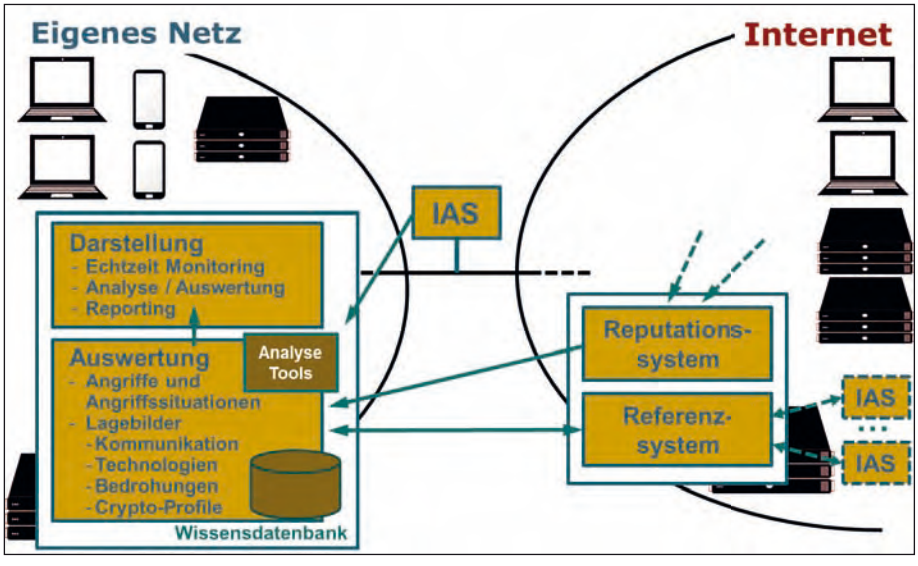


Abb. 2: Funktionsübersicht des Internet-Analyse-Systems

Ziele des Kommunikationslagebildes

Mithilfe des Kommunikationslagebildes können mehrere Ziele erreicht werden:

1. Erkennen von Angriffs- und Gefahrensituationen

Mithilfe einer Anomalie- oder Angriffssignaturerkennung werden Angriffs- und Gefahrensituationen aus den Kommunikationsmerkmalen identifiziert und dargestellt. Dies stellt oftmals den ersten Ansatz dar, um Ursprung und Ziel des Angriffes nach und nach einzugrenzen: Damit können im späteren Verlauf die relevanten Kommunikationsmerkmale zur Auswertung festgelegt werden.

2. Analyse und Auswertung der Angriffs- und Gefahrensituationen

Dank der Analyse und Auswertung der Angriffs- und Gefahrensituationen werden weitere Sichtweisen und Hilfestellungen umgesetzt, um ein besseres Verständnis über die Kommunikationslage zu erhalten. Auf Basis detaillierter Analysen bestimmter Angriffs- und Gefahrensituationen wird anhand eines Favoritensystems eine schnelle Übersicht mit den relevanten Kommunikationsmerkmalen erstellt. Das System ist dank einer Wissensdatenbank lernfähig. Es lässt Erfahrungen und bereits vergangene Angriffe in die Analyse einfließen, um schnell Abweichungen vom Normalzustand festzustellen.

3. Übersicht und Bewertung der Kommunikationslage

Um eine effektive Übersicht der Kommunikationslage zu erhalten, wird zum einen ein „Echtzeit-Monitoring" bereitgestellt, das den Ist-Zustand der Kommunikationslage grafisch darstellt. Zum anderen wird ein „Reporting" verwendet. Dieses führt eine Bewertung der Kommunikationslage mithilfe eines Reputationssystems durch, bei dem Parameter durch bekannte Reputationsdaten anhand eines Ampelsystems eingeordnet werden.

Funktionsübersicht des Internet-Analyse-Systems

In Abbildung 2 ist eine Funktionsübersicht des Internet-Analyse-Systems dargestellt.

1. Darstellung der Ergebnisse des Internet-Analyse-Systems

Mithilfe des „Echtzeit-Monitorings" wird der Ist-Zustand der Kommunikationslage

dargestellt. Damit ist es immer möglich, einen schnellen, intuitiven Überblick über die aktuelle Kommunikationslage zu bekommen (Quellen: /PoSp07/ und /PoSc10/).

Mit der „Analyse und Auswertung" können Angriffs- und Gefahrensituationen analysiert und ausgewertet werden, um die richtigen Entscheidungen treffen zu können.

Das „Reporting" hilft, regelmäßig eine strukturierte und bewertete Darstellung der Kommunikationslage zu erlangen, um auf dieser Basis eine mittelfristige Entscheidung für mehr Sicherheit treffen zu können. Die Reporte können in wählbaren zeitlichen Abständen abonniert und per E-Mail verteilt werden. Durch die Art der Verteilung können die intelligenten und übersichtlichen E-Mail-Reporte auch einfach weitergeleitet werden.

2. Auswertung

Das Internet-Analyse-System hat vielfältige Analyse-Tools, mit denen die unterschiedlichsten Berechnungen für die Angriffs- und Gefahrensituationen, Heuristiken von besonderen Darstellungen usw. umgesetzt werden können. Die Wissensdatenbank repräsentiert die Historie von Mess- und Analyseergebnissen.

3. Reputationssystem

Das Kommunikationslagebild zeigt auf, welche Technologien (zum Beispiel Browser, Betriebssysteme, Sicherheitstools), Anwendung von Verschlüsselung (zum Beispiel HTTPS, IMAPS, POP3S, SMTPS, IPSec), Verwendung von kryptographischen Profilen (zum Beispiel SSL/TLS) usw. verwendet werden. Mithilfe eines Reputationssystems werden diese Aspekte bewertet. Verwendete Browser, die nicht aktualisiert sind oder derzeit kritische Schwachstellen beinhalten, werden rot gekennzeichnet. Verwendete Browser, die aktuell sicher sind, werden grün dargestellt. Protokolle, die bekanntlich überwiegend für Angriffe verwendet werden, sind entsprechend rot gekennzeichnet. Das Gleiche gilt für verwendete Kryptoprofile, Sicherheitstechnologien und vieles mehr. Damit das Reputationssystem diese Bewertung umsetzen kann, werden die dazu notwendigen Informationen teilautomatisiert beschafft und in das Reputationssystem eingepflegt.

4. Referenzsystem (Globale Sichtweise)

Das Kommunikationslagebild zeigt auf, wie die Kommunikationsmerkmale, die für die Bewertung der Sicherheit über den positiven Kommunikationsablauf notwendig sind, genutzt werden. Beispiel: Ist die Identifikation von Scan-Angriffen auf Port 80 (HTTP) von 130 Prozent normal oder die Basis eines gezielten Angriffes? Wenn bei solchen Werten Referenzwerte von anderen Organisationen (zum Beispiel insgesamt in Deutschland, in bestimmten Branchen …) zur Verfügung stünden, dann könnten eigene Ergebnisse besser bewertet werden. Aus diesem Grund ergibt sich die Idee der globalen Sichtweise: Organisationen tauschen wichtige Kommunikationsmerkmale anonymisiert in einer Zentrale aus, die diese Werte statistisch berechnet und wieder an alle verteilt – sie stehen dann als Referenzwerte für die eigene Bewertung zur Verfügung. Dies geschieht immer vollständig anonym.

Beispiele für die Bewertung der Kommunikationslage

Die Kommunikationslage stellt die reale Nutzung von aktuell verwendeten Technologien und Internet-Protokollen dar. Eine große Gefahr entsteht erst durch die Nutzung veralteter oder nicht aktualisierter Software, wie beispielsweise Betriebssysteme, Browser oder Sicherheitstools, da sie Angreifern oft als Einfallstor dienen. Gerade für Unternehmen, deren Mitarbeiter die eigenen Geräte zur Arbeit nutzen, ist schwer nachzuhalten, welche Software tatsächlich verwendet wird und welche potenziellen Bedrohungen sich außerdem auf diesen Geräten befinden. Das IAS stellt dar, wie viele dieser Lücken an welcher Stelle vorhanden sind. Es wird auch erfasst, ob überhaupt verschlüsselt wird und welche kryptographischen Profile dabei genutzt werden. Dazu wird das Reputationssystem genutzt, welches Aussagen über die Sicherheit von Protokollen, Technologien, Kryptoprofilen etc. zur Verfügung stellt. Im Laufe der NSA-Affäre wurde festgestellt, dass nicht alle Technologien die gleiche Sicherheit mitbringen. Der fahrlässige Umgang mit sensiblen Daten und die Verwendung unsicherer Verschlüsselungstechnologien ist eines der größten Probleme bei Wirtschaftsspionage. Das IAS hilft somit, das Risiko von Spionage und Datenklau stark einzuschränken.

Das BSI empfiehlt zurzeit die Nutzung der TLS-/SSL-Version 1.2 (Beispiel für eine Referenz). In Abbildung 3 sehen wir jedoch, dass bei diesem Netzwerk mehr als 50 Prozent diese Sicherheitstechnologie noch nicht nutzen. Mit dieser Information kann die Lage nun definiert und ein Technologiewechsel umgesetzt werden, um das Risiko zu minimieren.

In Abbildung 4 wird beispielsweise ersichtlich, dass die „Protocol number 50 (ESP Mode von IPSec)" zu 0,8 Prozent verwendet wird. Dies bedeutet, dass jedes 125ste IP-Paket IPSec-verschlüsselt wird.

TLS - Version	Pakete	
	Anzahl	%
SSL Version SSL 2.0	0	0,00
SSL Version SSL 3.0	25.989	0,12
SSL Version TLS 1.0	10.154.344	48,42
SSL Version TLS 1.1	608.026	2,90
SSL Version TLS 1.2	10.182.293	48,55
SSL Version Other	0	0,00
Gesamt	**20.970.652**	**100,00**

Abb. 3: Genutzte TLS-/SSL-Technologie

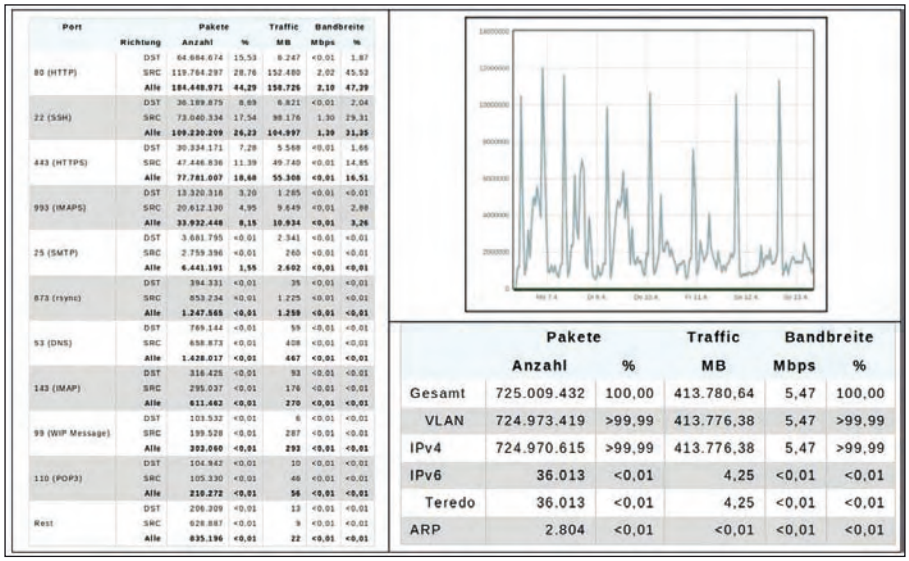
Nutzung und Verteilung von aktuell verwendeten Internet-Protokollen

Mithilfe des Kommunikationslagebildes können wir die Nutzung und Verteilung der Internet-Protokolle darstellen. Hier einige Beispiele.

In Abbildung 5 ist der sehr dominante Wochenverlauf des Kommunikationsmerkmals IPv4 zu erkennen. Neben dem typischen Tagesverlauf ist auch erkennbar, dass der Verkehr am Wochenende geringer ausfällt. Unten rechts ist die Nutzung von IPv4, IPv6 und ARP zu erkennen. Hier werden die Anzahl der identifizierten Pakete, der Traffic in MByte und die Bandbreite dargestellt. Links kann die Verteilung der Anwendungsprotokolle analysiert werden. Port 80 (HTTP) ist mit 47 Prozent das meistgenutzte Protokoll. DST und SRC geben einen Hinweis darüber, wie viele Pakete vom Netzwerk in das Internet gesendet worden sind und wie viele vom Internet in das Netzwerk übertragen wurden.

IP Protokollnummer	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Protocol number 6 (TCP)	468.472.020	64,62	358.462	4,74	86,63
Protocol number 17 (UDP)	237.139.295	32,71	53.729	0,71	12,99
Protocol number 1 (ICMP)	18.914.729	2,61	1.582	0,02	0,38
Protocol number 50 (ESP)	5.799.799	0,8	<1	<0,01	<0,01
Protocol number 2 (IGMP)	4.431	<0,01	2	<0,01	<0,01
Protocol number 132 (SCTP)	12	<0,01	<1	<0,01	<0,01
Protocol number 46 (RSVP)	1	<0,01	<1	<0,01	<0,01
Rest	0	0,00	0	0,00	0,00
Gesamt	**724.974.918**	**100,00**	**413.776**	**5,47**	**100,00**

Abb. 4: Verteilung der IP-Portnummern



	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Gesamt	725.009.432	100,00	413.780,64	5,47	100,00
VLAN	724.973.419	>99,99	413.776,38	5,47	>99,99
IPv4	724.970.615	>99,99	413.776,38	5,47	>99,99
IPv6	36.013	<0,01	4,25	<0,01	<0,01
Teredo	36.013	<0,01	4,25	<0,01	<0,01
ARP	2.804	<0,01	<0,01	<0,01	<0,01

Abb. 5: Nutzung und Verteilung von Protokollen

Traffic-Art	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Src >= 1024 and Dst >= 1024 ("P2P") - client-to-client	49.922.825	10,66	23.096	0,31	6,44
Src < 1024 and Dst < 1024 ("B2B") - server-to-server	326.388	0,07	22	<0,01	<0,01
Src >= 1024 and Dst < 1024 ("P2B") - client-to-server	152.183.466	32,49	22.752	0,30	6,35
Src < 1024 and Dst >= 1024 ("B2P") - server-to-client	266.037.102	56,79	312.589	4,13	87,20
Gesamt	**468.469.781**	**100,00**	**358.458**	**4,74**	**100,00**

Abb. 6: Nutzung und Verteilung von Übertragungsarten

Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar

Mit Abbildung 6 werden Traffic-Arten mithilfe einer Heuristik berechnet und dargestellt. Server-to-Client zeigt die Angabe vom Server zum Client und Client-to-Server die umgekehrte Richtung. Client-to-Client stellt eine Peer-to-Peer-Kommunikation dar. Dies könnte beispielsweise der illegale Download von Inhalten sein.

Besondere Eigenschaften des Internet-Analyse-Systems

Die IAS-Sonden liefern eine Übersicht der Netzwerkaktivitäten und werten den Datenverkehr von einer rein passiven Position aus. Um mögliche Bedenken auszuräumen: Diese Sondentechnologie ist als deutsches Open-Source-Produkt des if(is) ohne eingebaute Hintertüren und steht zur freien Einsicht im Internet zur Verfügung. Es hält sich an die Vorgaben des Qualitätszeichens „IT Security made in Germany" und erfüllt das passende Common-Criteria-Profil. Zudem ist der Datenschutz seit Beginn des Internet-Analyse-Systems ein sehr wichtiges Thema und Bestandteil der Entwicklung: Es ist nicht möglich, Netzteilnehmer in irgendeiner Form zu überwachen oder Rückschlüsse mithilfe von Profilbildung auf Verhalten oder Metadaten zu ziehen. Das Surfverhalten einzelner Nutzer wird nicht aufgezeichnet, eine Mitarbeiterüberwachung ist ausgeschlossen. Die Grundlage dafür wurde auch in Zusammenarbeit mit dem Bundesdatenschutzbeauftragten und dem Landesdatenschutzbeauftragten NRW erarbeitet. Aus diesen Gründen vertraut das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf das Internet-Analyse-System und nutzt es im Regierungsnetz.

Vertrauen ist gut – Kontrolle ist besser

In der wirtschaftlichen Realität wird in vielen Unternehmen die eigene IT-Infrastruktur aus finanziellen oder firmenpolitischen

Gründen durch externe Dienstleister betrieben und gewartet. Diese Dienstleister gehen in den Firmen ein und aus. Sie übernehmen vertraglich die Verantwortung für die IT-Sicherheit und den reibungslosen Betrieb der hausinternen IT, der eigenen Server oder gar des ganzen Rechenzentrums. Hier bietet das Internet-Analyse-System einen großen Mehrwert: Denn Vertrauen ist gut, aber Kontrolle ist besser. Mit dem IAS lässt sich auch die Arbeit der externen IT-Dienstleister kontrollieren, wodurch die Prüfung der Umgebung und der Gegebenheiten auf IT-Sicherheit und die Erfüllung der getroffenen Vereinbarungen möglich ist.

Teilnahme an einem Pilotprojekt

Das Institut für Internet-Sicherheit wird ein Pilotprojekt mit dem Internet-Analyse-System und interessierten Organisationen durchführen. Es fallen keine Kosten für die IAS-Software an, welche quelloffen zur freien Verfügung steht. Es muss lediglich die je nach Anforderung handelsübliche Hardware als Basis für den Betrieb der Software zur Verfügung gestellt werden. Der Betrieb ist kaum mit Wartungsaufwand verbunden und funktioniert praktisch „Out-of-the-Box".

Der Kostenaufwand für das eigene Unternehmen ist somit sehr gering: ein PC plus Strom. Die „Bezahlung" für die Nutzung des Internet-Analyse-Systems erfolgt durch die Bereitstellung der gesammelten, anonymen Daten. Es profitieren alle Unternehmen erheblich durch den dadurch ermöglichten Vergleich der Daten.

Ziele des Internet-Analyse-Systems

Das Ziel ist klar definiert: Es sollen die Kommunikationsrisiken für eine Vielzahl von Unternehmen identifiziert und damit das eigene Risiko minimiert werden. In der heutigen Zeit steigender Bedrohungen ist eine großflächige Zusammenarbeit der Betroffenen unabdingbar geworden. Daher richtet sich das Internet-Analyse-System nicht nur an einzelne Unternehmen, sondern spricht sich gezielt für eine gemeinsame Allianz von vielen aus. Bei der Zusammenarbeit möglichst zahlreicher Partnerunternehmen/-Organisationen ergibt sich ein deutlich geringeres Risiko und damit auch weniger finanzieller Aufwand für jeden Einzelnen. Zudem wird erst dadurch ein anonymer Vergleich der Berechnung hilfreicher Referenzwerte möglich. Durch die Auswertung der Nutzungs- und Bedrohungsdaten aller Teilnehmer ist die Berechnung globaler Kommunikationsrisiken möglich. Das if(is) kann durch das Internet-Analyse-System über die Zeit hinweg immer präzisere Hilfestellungen anbieten und Maßnahmen empfehlen. Das IAS ermöglicht somit eine höhere IT-Sicherheit sowohl für die teilnehmenden Unternehmungen als auch für die Allgemeinheit.

Das Internet-Analyse-System soll zudem immer weiter entwickelt werden, um ein breiteres Spektrum an potenziellen Risiken zu erkennen und auch zukünftigen Bedrohungen zu begegnen. So wird an einer Anwendungserkennung, auch von verschlüsselten Daten, gearbeitet, und auch die Erkennung von Botnetzen soll in Zukunft integriert werden. Die weitere Entwicklung des IAS ist aber vor allem von den Daten der nutzenden Unternehmen abhängig. Auf diese Ergebnisse soll reagiert werden, um das IAS flexibel in Richtung der Anforderungen weiterzuentwickeln. Damit wird der Mehrwert für alle Beteiligten steigen und das IAS zu einer zukunftssicheren IT-Sicherheitstechnologie werden.

Zusammenfassung

Die IT-Sicherheitsprobleme steigen ständig und damit auch das Risiko eines Schadens. Mithilfe eines Kommunikationslagebildes wird es möglich sein, den Gesundheitszustand des eigenen Netzwerkes und der daran angeschlossenen IT-Systeme zu analysieren und zu bewerten. Dies gemeinsam zu tun, wird die Effizienz steigern und die eigenen Risiken reduzieren. ■

Literatur

- */PoSp07/ N. Pohlmann, S. Spooren: „Darstellung von komplexen Sicherheitssituationen mit ‚Visual Internet Sensor Information (VisiX)' – Dem Internet den Puls fühlen", erschienen in der IT-SICHERHEIT 02/2007, S. 50-51, DATAKONTEXT-Fachverlag.*
- */PePo11/ D. Petersen, N. Pohlmann: „Ideales Internet-Frühwarnsystem", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 02/2011.*
- */PoSc10/ N. Pohlmann, A. Schnapp: „Gefahrenpotenzial visualisieren: Erfassung und Visualisierung des Malware-Aufkommens im World Wide Web", erschienen in der IT-SICHERHEIT 02/2010, S. 54-56, DATAKONTEXT-Fachverlag.*

DOMINIQUE PETERSEN,
Wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen und seit Januar 2007 Projektleiter des Bereichs Internet-Frühwarnsysteme

NORBERT POHLMANN,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen. Außerdem ist er Studienbeauftragter für den Master Internet-Sicherheit.

(1) *Siehe auch: http://www.internet-sicherheit.de/forschung/aktuelle-forschungsprojekte/internet-fruehwarnsysteme/internet-analyse-system/uebersicht/*