Die Kommunikationslage

Gefahr erkannt, Gefahr gebannt

Die IT-Sicherheitsereignisse aus jüngster Vergangenheit haben weitreichende Auswirkungen für alle Menschen und Unternehmen: 50 Milliarden Euro Schaden im Jahr im Bereich Wirtschaftsspionage laut den Aussagen aus dem Bundesinnenministerium, allein in Deutschland. Angriffe auf kritische Infrastrukturen und damit prinzipiell höhere Angreifbarkeit unserer Gesellschaft. 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. Es gibt jeden Tag eine steigende Anzahl an erfolgreichen Angriffen, sowohl im Bereich Software (Heartbleed, Windows XP, Schwachstellen in Browsern, Betriebssystemen und Anwendungen, usw.) als auch im Bereich von Hardware (datensammelnde Smart-TVs, Lücken in Routern, ausspähende Bügeleisen und Computermäuse, usw.). In vielen Branchen und Bereichen macht sich ein Ohnmachtsgefühl breit. Zu groß scheinen die Ausmaße an IT-Sicherheitsproblemstellen und -lücken zu sein, um etwas dagegen unternehmen zu können, zu beschränkt sind die derzeitig vorhandenen Möglichkeiten, um den Bedrohungen angemessen zu begegnen. Dennoch gibt es Strategien, die helfen, die Risiken nachhaltig zu reduzieren.

Die Herausforderung dabei ist, 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.

Erkennen von Gefahren

Die größte Gefahr besteht immer dann, wenn Bedrohungen falsch eingeschätzt werden. Wer die Gefahren hingegen kennt, kann sich und seine Werte besser schützen (siehe die Idee in Abbildung 1). Mit Hilfe eines Kommunikationslagebildes sollen Angriffe auf die IT-Systeme und Werte (also die Daten) einer Organisation erkannt sowie Schwachstellen der benutzten Technologien und Internet-Protokolle aufgezeigt werden. So lässt sich ein wirkungsvolles und nachhaltiges Schutzkonzept entwickeln.

Dies wird ermöglicht mit den drei wichtigsten Kernaspekten:

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.

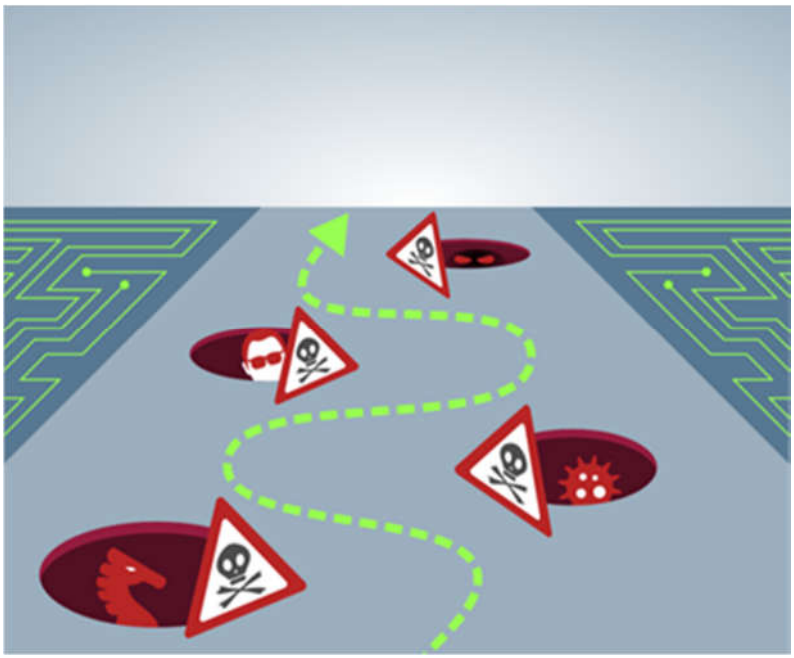


Abb. 1: Gefahr erkennt, Gefahr gebannt

Generierung eines Kommunikationslagebildes

In unserem Beispiel wird ein vollständiges Kommunikationslagebild mit Hilfe des Internet-Analyse-Systems (IAS) unter Verwendung eines speziellen IAS-Sensors ermittelt, der in der Regel zwischen dem Unternehmensnetzwerk und dem Internet positioniert ist. Der Sensor ist in der Lage, bis zu 3.000.000 potenzielle Kommunikationsmerkmale in den Kommunikationspaketen zu identifizieren und dann zu zählen. Das funktioniert wie bei einer Strichliste. Wenn das Kommunikationsmerkmal festgestellt wird, dann wird dieses gezählt. Ein Kommunikationsmerkmal kann ein Kommunikationsparameter oder eine Verknüpfung von verschiedenen Kommunikationsparametern sein. In der Abb. 2 sind exemplarisch IPv6, IPv4, TCP, UDP, http, HTTPS und SMTP, sieben der 3.000.000 möglichen Kommunikationsmerkmale dargestellt (siehe auch: http://www.internet-sicherheit.de/forschung/aktuelle-forschungsprojekte/internet-fruehwarnsysteme/internet-analyse-system/uebersicht/) .

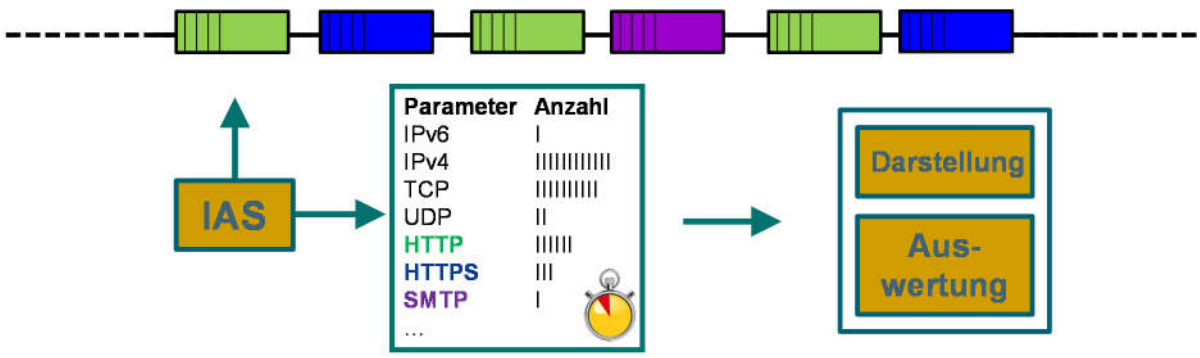


Abb. 2: Prinzip der Extrahierung der sicherheitsrelevanten Informationen

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 Grad der Reduzierung 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 5 min. ideale Werte erbringt. Bei einer typischen IAS-Sonde werden so ca. 10 G Byte Daten pro Jahr gesammelt. Das Prinzip der Ermittlung der Kommunikationsmerkmale ist dabei datenschutzkonform. Das heißt, es werden keine Nutzerdaten, IP-Adressen oder sonstige personenbezogenen oder -beziehbare Informationen bewertet /PePo11/.

Die Kommunikationsmerkmale zeigen dabei sicherheitsrelevante Informationen über verschiedene Aspekte wie Angriffe (Ports, SYS-ACK, usw.), genutzte Technologien (User-Agent, Versionen von Technologien und Standards, usw.) und die Nutzung/Verteilung von Protokollen und Anwendungen an. Dadurch erlauben sie, 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 beteilig 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.

Ziele des Kommunikationslagebildes

Mit der Hilfe des Kommunikationslagebildes können mehrere Ziele erreicht werden:

1.) Erkennen von Angriffs- und Gefahrensituationen
Mit Hilfe 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 u. 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 u. 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 mit Hilfe eines Reputationssystems durch, bei dem Parameter durch bekannte Reputationsdaten anhand eines Ampelsystems eingeordnet werden.

Funktionsübersicht des Internet-Analyse-Systems

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

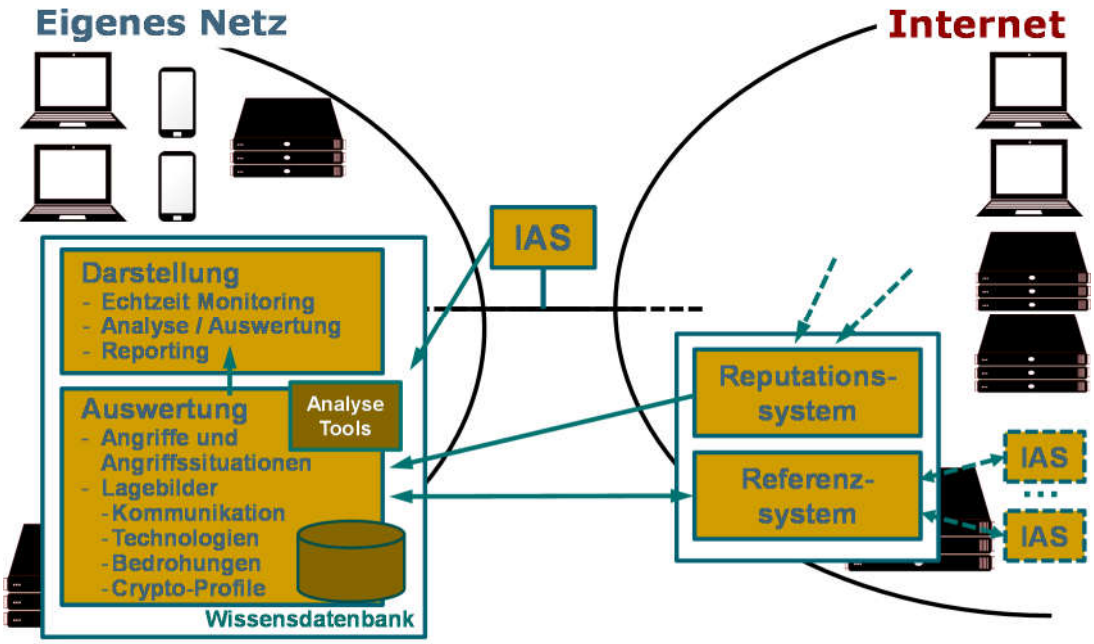


Abb. 3: Funktionsübersicht des Internet-Analyse-Systems

1.) Darstellung der Ergebnisse des Internet-Analyse-Systems

Mit Hilfe 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 /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 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 (Browser, Betriebssysteme, Sicherheitstools, …), Anwendung von Verschlüsselung (HTTPS, IMAPS, POP3S, SMTPS, IPSec, …), Verwendung von kryptographischen Profilen (SSL/TLS, …), usw. verwendet werden. Mit Hilfe 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, usw. 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 einen klaren Sachverhalt über die Nutzung von Kommunikationsmerkmalen, die für die Bewertung der Sicherheit über den positiven Kommunikationsablauf notwendig sind. Bei der Identifizierung von besonderen Situationen, wie Angriffen, Gefahren und sonstigen Besonderheiten, fällt es aber oft sehr schwer, eine richtige Einschätzung durchführen zu können. Beispiel: Ist die Identifikation von Scan-Angriffen auf Port 80 (HTTP) von 130 % normal oder die Basis eines gezielten Angriffes? Wenn bei solchen Werten Referenzwerte von anderen Organisationen (z.B. 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 aus, in einer Zentrale, die diese Werte statistisch berechnet und wieder an alle verteilt. Diese stehen dann als Referenzwerte für die eigene Bewertung zur Verfügung. Dies geschieht immer vollständig anonym.

Beispiele für die Bewertung der Kommunikationslage

Nutzung und Verteilung von aktuell verwendeten Technologien

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 zum Beispiel Betriebssysteme, Browser, Sicherheitstools, usw., da sie oft Einfallstore für Angreifer bieten. Gerade für Unternehmen, deren Mitarbeiter ihre eigenen Geräte zur Arbeit benutzen, ist schwer nachzuhalten, welche Software tatsächlich verwendet wird und was sich noch alles für potenzielle Bedrohungen 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, Crypto-Profilen usw., 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.

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. 4: Genutzte TLS/SSL Technologie

Das BSI empfiehlt zurzeit die Nutzung der TLS/SSL Version 1.2 (Beispiel für eine Referenz). In Abb. 4 sehen wir aber, dass bei diesem Netzwerk mehr als 50 % diese Sicherheitstechnologie noch nicht nutzen. Mit dieser Information kann die Lage nun definiert und ein Technologiewechsel umgesetzt werden, um das Risiko zu minimieren.

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**

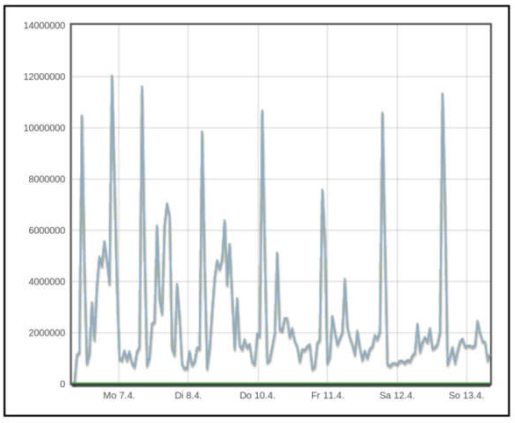
Abb. 5: Verteilung der IP Portnummern

In Abb. 5 wird z.B. ersichtlich, dass die „Protocol number 50 (ESP Mode von IPSec)“ zu 0,8 % verwendet wird. Dies bedeutet, dass jedes 125. IP Paket IPSec verschlüsselt wird.

Nutzung und Verteilung von aktuell verwendeten Internet-Protokollen

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

Port	Richtung	Pakete Anzahl	Pakete %	Traffic MB	Bandbreite Mbps	Bandbreite %
80 (HTTP)	DST	64.684.674	15,53	6.247	<0,01	1,87
	SRC	119.764.297	28,76	152.480	2,02	45,53
	Alle	**184.448.971**	**44,29**	**158.726**	**2,10**	**47,39**
22 (SSH)	DST	36.189.875	8,69	6.821	<0,01	2,04
	SRC	73.040.334	17,54	98.176	1,30	29,31
	Alle	**109.230.209**	**26,23**	**104.997**	**1,39**	**31,35**
443 (HTTPS)	DST	30.334.171	7,28	5.568	<0,01	1,66
	SRC	47.446.836	11,39	49.740	<0,01	14,85
	Alle	**77.781.007**	**18,68**	**55.308**	**<0,01**	**16,51**
993 (IMAPS)	DST	13.320.318	3,20	1.285	<0,01	<0,01
	SRC	20.612.130	4,95	9.649	<0,01	2,88
	Alle	**33.932.448**	**8,15**	**10.934**	**<0,01**	**3,26**
25 (SMTP)	DST	3.681.795	<0,01	2.341	<0,01	<0,01
	SRC	2.759.396	<0,01	260	<0,01	<0,01
	Alle	**6.441.191**	**1,55**	**2.602**	**<0,01**	**<0,01**
873 (rsync)	DST	394.331	<0,01	35	<0,01	<0,01
	SRC	853.234	<0,01	1.225	<0,01	<0,01
	Alle	**1.247.565**	**<0,01**	**1.259**	**<0,01**	**<0,01**
53 (DNS)	DST	769.144	<0,01	59	<0,01	<0,01
	SRC	658.873	<0,01	408	<0,01	<0,01
	Alle	**1.428.017**	**<0,01**	**467**	**<0,01**	**<0,01**
143 (IMAP)	DST	316.425	<0,01	93	<0,01	<0,01
	SRC	295.037	<0,01	176	<0,01	<0,01
	Alle	**611.462**	**<0,01**	**270**	**<0,01**	**<0,01**
99 (WIP Message)	DST	103.532	<0,01	6	<0,01	<0,01
	SRC	199.528	<0,01	287	<0,01	<0,01
	Alle	**303.060**	**<0,01**	**293**	**<0,01**	**<0,01**
110 (POP3)	DST	104.942	<0,01	10	<0,01	<0,01
	SRC	105.330	<0,01	46	<0,01	<0,01
	Alle	**210.272**	**<0,01**	**56**	**<0,01**	**<0,01**
Rest	DST	206.309	<0,01	13	<0,01	<0,01
	SRC	628.887	<0,01	9	<0,01	<0,01
	Alle	**835.196**	**<0,01**	**22**	**<0,01**	**<0,01**



	Pakete Anzahl	Pakete %	Traffic MB	Bandbreite Mbps	Bandbreite %
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

In Abb. 5 rechts oben ist der sehr dominante Wochenverlauf des Kommunikationsmerkmales IPv4 zu erkennen. Der typische Tagesverlauf ist erkennbar, aber auch, 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 Bandreite dargestellt. Links kann die Verteilung der Anwendungsprotokolle analysiert werden. Port 80 (HTTP) ist mit 47 % das meist genutzte Protokoll. DST und SRC geben einen Hinweis darüber, wieviel Pakete vom Netzwerk in das Internet gesendet worden sind und wie viele vom Internet in das Netzwerk übertragen wurden.

Traffic-Art	Pakete Anzahl	Pakete %	Traffic MB	Bandbreite Mbps	Bandbreite %
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

In Abb. 6 werden Traffic-Arten mit Hilfe 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 z.B. das illegale Downloaden 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 Bedenken im Voraus auszuräumen: Diese Sondentechnologie ist ein deutsches Open-Source-Produkt des Instituts für Internet-Sicherheit - 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 von Beginn des Internet-Analyse-Systems an ein sehr wichtiges Thema gewesen und Bestandteil der Entwicklung: Es ist nicht möglich, Netzteilnehmer in irgendeiner Form zu überwachen oder Rückschlüsse mit Hilfe von Profilbildung auf Verhalten oder Metadaten zu ziehen. Das Surfverhalten einzelner Nutzer wird nicht aufgezeichnet, eine Mitarbeiterüberwachung ist ausgeschlossen. Die Grundlage dafür wurden auch in Zusammenarbeit mit dem Bundesdatenschutzbeauftragtem und dem Landesdatenschutz NRW erarbeitet. Aus diesen Gründen vertraut auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf das Internet-Analyse-System und nutzt es im Regierungsnetz.

Vertrauen ist gut, aber 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 und 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. Die Prüfung der Umgebung und der Gegebenheiten auf IT-Sicherheit und die Erfüllung der getroffenen Vereinbarungen sind dadurch möglich.

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, sondern es muss lediglich die je nach Anforderung handelsübliche Hardware als Basis für den Betrieb der Software zur Verfügung

gestellt werden (siehe Abb. 7). Der Betrieb ist kaum mit Wartungsaufwand verbunden und funktioniert praktisch "Out-of-the-Box".

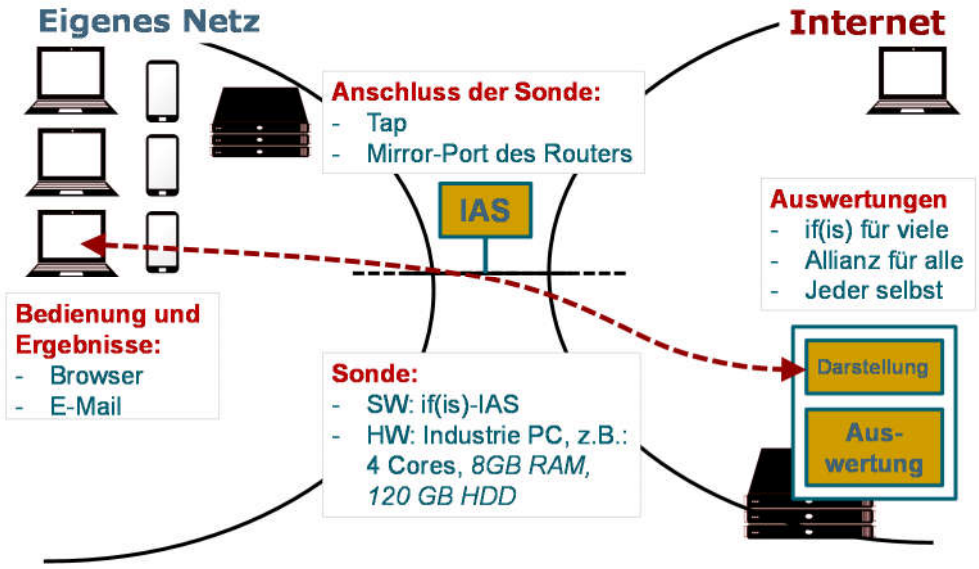


Abb. 7: Teilnahme am Pilotprojekt

Der Kostenaufwand für das eigene Unternehmen ist somit sehr gering: Ein PC plusStrom. 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.

Die 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 vieler 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 weiter zu entwickeln. 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. Mit Hilfe 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 „VisiX“ - Dem Internet den Puls fühlen“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 02/2007

/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: Erfassen und Visualisierung des Malware-Aufkommens im World Wilde Web“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 2/2010

Autoren:

Dominique Petersen

Wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit 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.