Frühwarnungen und Verfügbarkeitsüberwachung

Nationales Lagezentrum für IT-Gefahren geplant

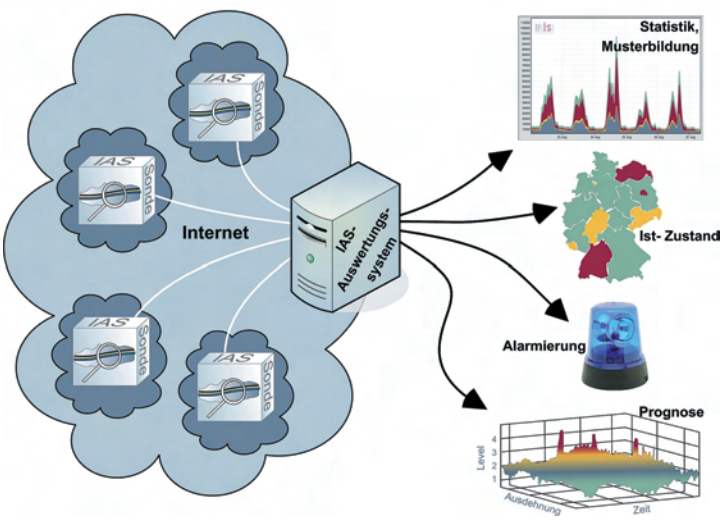
Auf der Datenautobahn, dem Internet und den einzelnen Unternehmensnetzen, finden sich heute ähnliche Probleme wie auf Verkehrswegen. Es drohen Staus, Unfälle, Verspätungen, Kosten und es fehlt der rechte Überblick. Nun ist ein Frühwarnsystem absehbar, das hilft, „Verkehrsgefährdungen" im Netz frühzeitig zu erkennen, um unternehmerische und behördliche Abläufe zu schützen.

Von Mathias Deml, Malte Hesse, Markus Linnemann und Norbert Pohlmann

Da das Internet sich zu einer wichtigen – und Kritischen – Infrastruktur entwickelt hat, wurde 2005 in Deutschland ein Nationaler Plan zum Schutz der Informationsinfrastrukturen[1] in Auftrag gegeben. Dieser Plan schreibt die Einrichtung eines Krisenreaktionszentrums vor, das im Sinne eines Lagezentrums ein

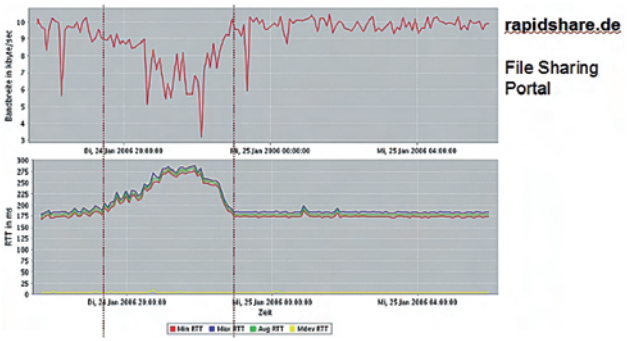
- Lagebild über den Zustand und die aktuelle Bedrohungslage im Internet liefern kann,
- Handlungsempfehlungen herausgibt und
- Frühwarnungen generiert oder reaktive Maßnahmen einleitet.

Anders als bei anderen kritischen Infrastrukturen fehlt eine zentrale Überwachung und die Regulierungsdichte für das Medium „Internet" ist weitaus geringer. Bei einer kontinuierlichen Analyse der Bedrohungslage ließe sich beispielsweise erkennen, ob gezielte Angriffe auf Grund einer bestimmten Schwachstelle zu erwarten sind. Insbesondere durch rechtzeitige Frühwarnungen können „Verwalter" der kritischen Infrastruktur dann auf die betreffende Gefahr fokussiert werden. Mithilfe konkreter Handlungsempfehlungen, zum Beispiel das Einspielen eines Sicherheitsupdates, wird der Schaden dann verhindert oder reduziert.



Dass Frühwarnungen sinnvoll sind, zeigte sich beispielsweise im Juli 2008, als US-CERT, rechtzeitig bevor große Schäden entstehen konnten, vor einem massives Sicherheitsproblem des DNS-Dienstes[2] warnte. Dieses Problem wurde selbst von den Redakteuren der klassischen Massenmedien als so gravierend eingestuft, dass es zu einer breiten Berichterstattung kam. Insgesamt muss man festhalten, dass der Schutz von kritischen Infrastrukturen jedem einzelnen Mitgliedsstaat der Europäischen Union selbst obliegt. Dabei kann sich der Deutsche Staat nicht drauf verlassen, dass eine der vorhandenen öffentlichen oder privaten Institutionen vor wichtigen Bedrohungen warnen, sondern die Verantwortlichen investieren aktiv in den Schutz der Bürger. Darüber hinaus müssen Konzepte erarbeitet werden, die einen effizienten und verlässlichen Austausch von Informationen und Handlungsempfehlungen zwischen allen Beteiligten erlauben.

In der Praxis gibt es jedoch einige Hürden für eine perfekte Umsetzung der

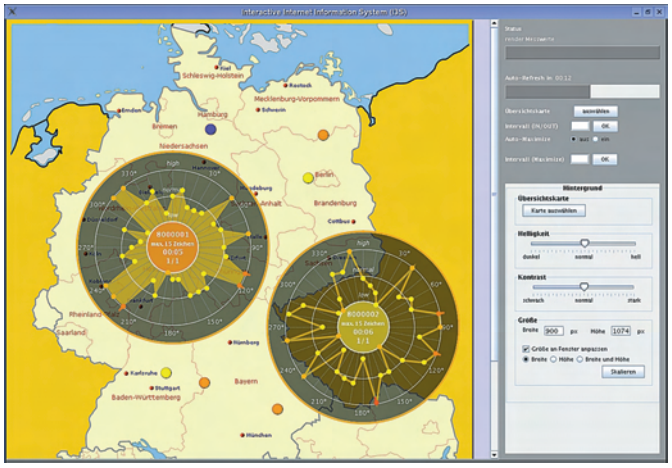


genannten Ziele. Die wichtigste: Das Internet ist heute ein Zusammenschluss von mehr als 27.000 eigenständig verwalteten autonomen Systemen[3], bei dem jeder Netzbetreiber nur eine eingeschränkte Sicht auf seinen eigenen „kleinen“ Ausschnitt des Netzes hat. Ein perfektes nationales Lagezentrum müsste aber möglichst all jene Netze erfassen, die eine hohe Relevanz für das „deutsche Internet“ haben. Auf Grund der Wettbewerbssituation zwischen den Netzbetreibern ist aber verständlich, dass zumindest Unternehmen ihre Daten nicht preisgeben. Die Anforderungen an ein Frühwarnsystem müssen also erweitert werden: Die Verarbeitung der Informationen muss konform mit den Ansprüchen der beteiligten Unternehmen an die Vertraulichkeit ihrer Daten erfolgen.

Im Rahmen von Forschung und Entwicklung wird im Institut für Internet-Sicherheit insbesondere in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik derzeit ein Frühwarnsystem aufgebaut, das ein Netzwerk überwachen kann, ohne die Vertraulichkeit zu verletzen. Dazu war auch die Entwicklung eines sonden-basierten Internet-Analyse-Systems und eines Internet-Verfügbarkeits-Systems nötig.

Im **Internet-Analyse-System (IAS)** werden kontinuierlich Messdaten erhoben, automatisiert bewertet und in das Lagebild einbezogen. Es basiert auf einer passiven Sensortechnologie (Sonden), die kontinuierlich statistische Rohdaten aus Headerinformationen des beobachteten Netzwerkverkehrs an ausgewählten Positionen der Infrastruktur sammelt. Personenbezogene und strategische Daten werden dabei nicht erfasst und Sitzungen einzelner Benutzer nicht verfolgt, so dass es zu keinen datenschutzrechtlichen Problemen oder zu Verletzungen der Vertraulichkeit kommt. Zurzeit ist das System in der Lage, mehr als 870.000 verschiedene Parameter zu erfassen, die schon heute für eine Angriffs- und Anomalieerkennung relevant sind[4] oder in der Zukunft einen wesentlichen Beitrag zum Erkennen von neuen Angriffen liefern könnten. Im zentralen Auswertesystem können für die Analyse notwendige Statistiken und Muster gebildet und der aktuelle Zustand der Infrastruktur visualisiert werden (Abb., S. 18). Mit Hilfe einer Prognosefunktion können zudem zukünftige Entwicklungen vorhergesagt und Frühwarnungen generiert werden (vgl. Abb. oben). Über Data-Mining Algorithmen [5] können Zusammenhänge zwischen Architekturen, Systemen und Protokollen erarbeitet werden, welche das Verständnis der zugrunde liegenden Infrastruktur fördern.

Das **Internet-Verfügbarkeits-System (IVS)** stellt mithilfe einer aktiven Sensortechnologie die Dienstgüte und Verfügbarkeit der wichtigsten Dienste im Internet und der Infrastruktur ▶



aus Benutzersicht dar. Mit den jeweils eingesetzten Protokollen wird versucht, bei den zu überwachenden Systemen eine Verbindung aufzubauen und den Dienst zu nutzen. Die Antwortzeiten werden gespeichert und dienen als Basis für das Lagebild. Durch Messungen verschiedener Dienstgüteparameter kann die aktuelle Leistungsfähigkeit der Netze beurteilt werden. Abbildung 4 zeigt exemplarisch mögliche Ergebnisse von Messungen. Hier wurde der HTTP-Dienst von rapidshare.de überwacht und als Dienstgüteparameter die Paketlaufzeit und verfügbare Bandbreite ermittelt. In der Zeit zwischen 18:00 und 23:00 Uhr lässt sich hier eine Verschlechterung der Bandbreite und längere Paketlaufzeiten ermitteln, was für eine erhöhte Nutzung des Dienstes in der gegebenen Zeit spricht.

Frühwarnsysteme im Unternehmen

Der nationale Plan sieht unter anderem vor, dass Behörden und Betreiber Kritischer Infrastrukturen in die Pflicht genommen werden, sicherheitskritische Vorfälle zu melden. Aber auch Unternehmen, die nicht an einem nationalen System teilnehmen, sind verpflichtet ihre Infrastrukturen im Rahmen eines Risikomanagements vor Schaden zu bewahren, denn für jedes Unternehmen ist die eigene IT-Infrastruktur ebenfalls eine Kritische. Die für das nationale Frühwarnsystem entwickelten Technologien lassen sich auch für ein effektives Frühwarnsystem im Unternehmen einsetzen. Sie gehen dabei über die Aufgaben von leistungsfähigen Intrusion Detection Systeme weit hinaus, deren Aufgabe die Erkennung von definierten Angriffssituationen ist. Durch die hohe Wertigkeit des Datenschutzes und der Vertraulichkeit von Unternehmensdaten schon während der Entwicklung der Technologie kann sie zukünftig als Basis zur unternehmensübergreifenden Überwachung durch den freiwilligen gegenseitigen Austausch von Daten und Warnungen verwendet werden, womit sich die Frühwarnung für alle Beteiligten weiter optimieren lässt.

Literatur

1 Bundesministerium des Inneren: Nationaler Plan zum Schutz der Informationsinfrastrukturen, 2005.
2 Heise: Massives DNS-Sicherheitsproblem gefährdet das Internet, 2008, http://www.heise.de/security/Massives-DNS-Sicherheitsproblem-gefaehrdet-das-Internet-/news/meldung/ 110641.
3 http://webapps.internet-sicherheit.de/aiconviewer/, 2008
4 Gianfranco Ricci, Betrachtung der vom IAS gesammelten Kommunikationsparameter auf Relevanz zur Anomalie und Angriffserkennung, Diplomarbeit, Fachhochschule Gelsenkirchen, 2008.
5 Svenja Wendler: Entwicklung eines Analysemoduls zum Internet-Analyse-System – Finden von Strukturen im Internetverkehr in Form von Assoziationsregeln, Diplomarbeit, Fachhochschule Gelsenkirchen, 2006.

Außerdem:
N. Pohlmann: „Probe-based Internet Early Warning System", ENISA Quarterly Vol. 3, No. 1, Jan-Mar 2007
N. Pohlmann: „Frühwarnsystem entdeckt Anomalien im Internetverkehr", Computer Zeitung, Nr. 3-4 / 22. Januar.
N. Pohlmann, M. Proest: „Die globale Sicht auf das Internet", iX – Magazin für professionelle Informationstechnik, Heise-Verlag, 2/2006

Über unsere Autoren:

Mathias Deml hat unlängst seine Abschlussarbeit im Bereich der Internet Erforschung abgeschlossen und arbeitet nun für eine Unternehmensberatung in Essen. Malte Hesse und Markus Linnemann sind wissenschaftliche Mitarbeiter am Institut für Internet-Sicherheit und Prof. Dr. Norbert Pohlmann ist geschäftsführender Direktor des Institutes für Internet-Sicherheit und Professor für verteilte Systeme und Informationssicherheit am Fachbereich Informatik der Fachhochschule Gelsenkirchen.
markus.linnemann@internet-sicherheit.de