Effektive Schadensbegrenzung

Internet-Frühwarnsysteme: Strukturen und Techniken

Was in der Erdbeben- und Hochwasserbeobachtung längst zum Standard gehört, sorgt auch im Internet für mehr Schadensbegrenzung. Frühwarnsysteme sollen aktuelle Zustände überwachen und möglichst früh vor drohenden Gefahren warnen. Frühwarnsysteme mit vergleichbaren Ansätzen können im Internet dazu führen, dass die Auswirkungen von zum Beispiel Viren, Würmern oder gezielten Sabotageakten verringert oder sogar gänzlich verhindert werden.

Durch die zunehmende Digitalisierung des sozialen und geschäftlichen Umfeldes steigt die Abhängigkeit von zuverlässigen elektronischen Kommunikationswegen. Daher ist das Internet als weltumspannendes Netzwerk mit seinen Diensten mehr und mehr als kritische Infrastruktur zu betrachten. Aus diesem Grund sind auch Internet Frühwarnsysteme nötig, mit deren Hilfe fundierte Aussagen über den Zustand dieser kritischen Infrastruktur getroffen werden können. Diese Internet- oder IT-Frühwarnsysteme sollten die Betroffenen über drohende Gefahren informieren und die Einleitung von Abwehrmaßnahmen ermöglichen, um so die schädlichen Auswirkungen hervorgerufen durch Viren, Würmer und gezielten Attacke verhindern.

Bedrohungslage Internet

Die Anzahl der bekannten Viren- und Wurmversionen steigt täglich - ihre Zahl hat die 100.000er Marke bereits im letzten Jahr überschritten und wächst monatlich um mehrere Hundert an. Die Hersteller von Antiviren- und Firewall-Software aktualisieren ihre Produkte teilweise mehrmals am Tag. Tools zur Einbruchserkennung und -vorbeugung (IDS / IPS) gehören längst zum Handwerkszeug von Security-Administratoren. Doch einen vollständigen Schutz mit absoluter Sicherheit kann und wird es nicht geben.

Neben experimentierfreudigen Jugendlichen, die mit selbst geschriebenen Viren und gezielten Sabotageakten ihre Netzwerkkenntnisse demonstrieren wollen und damit nicht unerheblichen Schaden anrichten, verzeichnen die Ermittlungsbehörden in zunehmendem Maße auch eine hohe Rate von Straftaten im Internet, die auf Industriespionage oder klassischen Delikten wie Erpressung und Betrug beruhen. Das Aufkommen dieser kriminellen Energien im Bereich Internet ist nicht neu, so wurden beispielsweise schon vor einiger Zeit Online-Wettbüros mit Attacken auf ihre Systeme erpresst. Dazu kommt das Problem des Versands von Spam-Mails über gekaperte Privat-PCs, Phishing-Attacken und viele andere Gefahren, denen der unbedarfte Internet-Benutzer nicht immer entsprechend begegnen kann.

Strukturen und Techniken eines Internet-Frühwarnsystems

Frühwarnsysteme im Internet sollen vom Prinzip her das gleiche leisten wie ihre Pendants im Bereich der Hochwasser-, Erdbeben- oder Staubeobachtung. Geschickt platzierte Messpunkte sammeln Daten, mit deren Hilfe sowohl die aktuelle Lage als auch daraus ableitbare zukünftige Situationen erkannt und vorhergesagt werden sollen. Diese Erkenntnisse sollen dabei helfen, die noch nicht Betroffenen möglichst früh und möglichst fundiert vor Bedrohungen und Gefahren zu warnen. Während im Bereich der Erdbebenfrühwarnung in Sekundenschnelle gehandelt werden muss, um eine Katastrophe beispielsweise durch brechende Gas-Pipelines zu verhindern, ist es im IT-Bereich nicht immer ganz klar, wie viel Zeit zwischen dem ersten Anzeichen für eine Gefahr und den spürbaren Auswirkungen liegt. Doch auch im Internet schrumpfen die Reaktionszeiten durch immer feinmaschigere Internet-Backbones und breitbandige DSL- oder Kabel-Anschlüsse auf Stunden und Minuten. Neue Viren- und Wurmgenerationen verbreiten sich innerhalb von wenigen Stunden um die ganze Welt. Hier besteht ein wesentlicher Unterschied zu den klassischen Frühwarnsystemen, die meist nur eine lokal begrenzte Gefahr erkennen müssen.

Ein weiterer wichtiger Unterschied bei Internet-Frühwarnsystemen ist, dass diejenigen, die den Grund für die Frühwarnung auslösen (z.B. Viren-Schreiber), das Wissen und die Funktionsweite des Frühwarnsystems mit berücksichtigen können.

Um Frühwarnsysteme klassifizieren und einordnen zu können, ist das folgende Ebenen-Modell hilfreich:

Abbildung 1: Ebenen-Modell Frühwarnsystem

Sensorik-Ebene

Auf der Sensorik-Ebene ist die Sammlung der Messwerte angesiedelt. Im Internet sind hier die verschiedensten Möglichkeiten denkbar. Zum einen ist es möglich auf bereits bestehende Datensammlungen zurückzugreifen wie sie etwa in Form von Logfiles bei Web-Servern, Firewalls, Antivirensoftware, Einbruchserkennungssystemen oder aber als Netzfluss-Informationen aus Routern vorliegen. Frühwarnsysteme, die nach diesem Prinzip arbeiten sind bei-

spielsweise das Distributed Intrusion Detection System "DShield.org" (http://www.dshield.org) und das Symantec DeepSight Threat Management System (http://enterprisesecurity.symantec.de).
Zum anderen besteht die technische Möglichkeit, die Kommunikationspakete direkt aus der zu betrachtenden Leitung heraus auszuwerten. Die Hersteller und Forscher setzen gerade in diesem Bereich verstärkt auf ihre eigenen Entwicklungen mit ganz unterschiedlichen Ansätzen. Entscheidend ist hier die sorgfältige Verteilung der Sensoren. Nur wenn repräsentative oder regional beziehungsweise logisch eingrenzbare Messwerte zur Verfügung stehen, können qualifizierte Aussagen getroffen werden (siehe auch Internet-Deutschland [1]).

Auswertungsebene
Die Auswertungsebene setzt neben Rechenleistung und Speicherplatz auch geeignete Algorithmen voraus. Aus den gesammelten Messwerten müssen Zustände erkannt und Statistiken generiert werden können. Dazu müssen Referenzdaten erzeugt und auf dem aktuellsten Stand gehalten werden. Vergleiche zwischen gegenwärtigen und früheren Zuständen müssen schnellstmöglich durchgeführt werden. Geeignete Algorithmen sollen es ermöglichen zwischen dem Normalzustand und einer erkannten Anomalie unterscheiden zu können. Des Weiteren ist die Erkennung von Anomalien anhand von charakteristischen Signaturen, die durch bereits erkannte Gefahren erlernt wurden, von großer Bedeutung. In diesem Umfeld ist noch erhebliche Forschungs- und Entwicklungsarbeit zu leisten.

Bewertungs- und Kategorisierungsebene
Der Ebene der Bewertung und Kategorisierung kommt ebenfalls eine große Bedeutung zu. Ist eine erkannte Unregelmäßigkeit auf ein normales Netzwerkverhalten zurückzuführen oder ist eine groß angelegte Cyber-Attacke die Ursache? Steigt die Last in einem bestimmten Bereich des Internets durch vermehrte Wurmaktivität oder stellt ein Hersteller lediglich ein neues Produkt-Update zur Verfügung, das von einer großen Anzahl von Nutzern gleichzeitig herunter geladen wird? Diese Bewertungen und Kategorisierungen sind nur schlecht zu automatisieren. Hier müssen Menschen Entscheidungen treffen, die durch ihr technisches Know-how, ihre Erfahrung und den Zugriff auf zusätzliche Informationen dazu befähigt sind.

Verbreitungsebene
Im Rahmen der Verbreitung der Informationen ist das geeignete Medium von hoher Bedeutung. So macht es beispielsweise wenig Sinn, die Betroffenen per E-Mail vor einer Bedrohung zu warnen, die große Teile der Internetstruktur bereits lahm gelegt hat, sodass die Warnungen ihr Ziel schon nicht mehr erreichen können. Hier müssen andere Wege, wie SMS oder Fax genutzt werden.

Auch sollten die Adressaten solcher Alarmmeldungen sorgfältig ausgewählt werden, denn bei nicht klar geregelter Verantwortlichkeit oder nicht genau definierten Kompetenzbereichen kann es passieren, dass die Alarmierung bei jemandem eintrifft, der nicht befugt ist, entsprechend zu reagieren beziehungsweise nicht das passende Know-how besitzt, um die notwendigen Maßnahmen einleiten zu können.

Realisierungsmöglichkeiten
Frühwarnsysteme, die den vorgenannten Kriterien entsprechen und die unterschiedlichsten Techniken implementieren, gibt es bereits am Markt. Sie werden zum einen als Dienstleistung angeboten, dass heißt die Kunden können beispielsweise über ein Web-Frontend in die gesammelten Daten Einblick nehmen und sich Analysen und Warnungen zusenden lassen. Die Anwender erhalten so eine globale Sicht des Internets. Zum anderen gibt es Frühwarnsysteme, die lokal im Netzwerk der Betreiber von Netzen installiert werden können und hier Frühwarnfunktionen bereitstellen. In diesem Fall fehlt dann natürlich eine globale Sichtweise und es können nur Anomalien im eigenen Netzwerk erkannt werden.
Hersteller und Dienstleister haben die Frühwarnsysteme und das ganzheitliche Bedrohungsmanagement als Geschäftsfeld entdeckt und bieten eine Vielzahl von Lösungen an. Doch auch die Open-Source-Gemeinde hat Lösungen entwickelt, die sich durchaus mit den kommerziellen Systemen messen können, unter anderem DShield.org.

Schlussbetrachtung und Ausblick
Eine große Anzahl von Gefahren bedroht die kritische Infrastruktur Internet täglich, und das in zunehmendem Maße. Frühwarnsysteme können den Verantwortlichen Werkzeuge an die Hand geben, mit deren Hilfe sich diese Gefahren abwenden lassen. Frühwarnsysteme gehören mehr und mehr fest zum Portfolio der Hersteller von Sicherheitssoftware und die Entwicklung der Systeme schreitet weiter voran. Das Institut für Internet-Sicherheit an der FH Gelsenkirchen entwickelt mit dem Internet-Analyse-System [2] und dem Internet-Verfügbarkeitssystem zwei eigene Lösungen im Bereich von IT-Frühwarnsystemen, die einen besonderen Ansatz in der Datenerhebung wählen. Nur wenn wir in der Lage sein werden, ein funktionierendes Internet-Frühwarnsystem aufzubauen, werden wir eine angemessene Verfügbarkeit des Internets erreichen können.

Stefan Korte
stefan.korte@internet-sicherheit.de
Prof. Dr. Norbert Pohlmann
norbert.pohlmann@informatik.fh-gelsenkirchen.de
Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
Neidenburger Str. 43
D - 45877 Gelsenkirchen
www.internet-sicherheit.de

Literatur
[1] S. Dierichs, N. Pohlmann: „Netz-Deutschland", iX - Magazin für professionelle Informationstechnik, Heise-Verlag, 12/2005
[2] N. Pohlmann: "Internetstatistik", Proceedings of CIP Europe 2005, Hrsg.: B.M. Hämmerli, S.D. Wolthusen; Gesellschaft für Informatik, Bonn 2005

Hinweis:
Zu dem Thema Identity Management wurde aus dem Artikel „Identitätskrisen in der IT" von Prof. Pohlmann und Markus Linnemann in der letzten Ausgabe der IT-SICHERHEIT ein Exzerpt abgedruckt. Den vollständigen Artikel finden Sie auf den Webseiten des if(is) Institut für Internet-Sicherheit unter:

www.internet-sicherheit.de/fileadmin/npo/artikel_berichte/Identity-Management-2005-11-17.pdf