CarmentiS

Auf dem Weg zu einem deutschen IT-Frühwarnsystem

Klaus-Peter Kossakowski, Jürgen Sander

PRESECURE Consulting GmbH
Beelertstiege 2
48143 Münster
kpk@pre-secure.de
js@pre-secure.de

Abstract: In diesem Kurzbeitrag wird das Projekt CarmentiS des deutschen CERT-Verbunds vorgestellt. Im Rahmen des Projekts wird eine Basisinfrastruktur für die Erprobung verfügbarer Ansätze und Strategien zur Ermittlung von zeitnahen Informationen über aktuelle Bedrohungslagen im deutschen Internet geschaffen.

1 Einleitung

Unsere Informationstechnik bietet mit ihrer zunehmenden Vernetzung eine Vielzahl von Angriffspunkten für feindliche Handlungen. Dies führt zu einer schleichend größer werdenden Bedrohung, die alle Bereiche der Wirtschaft, Industrie, der öffentlichen Verwaltung sowie die Privathaushalte betrifft. Herauszuheben ist indes sind Sektoren, die in der letzten Zeit als „kritische Infrastrukturen“ bezeichnet werden. Durch die Abhängigkeit vieler wichtiger Prozesse von funktionsfähigen IT- und TK-Systemen dieser Infrastrukturen, ist bei erheblichen Störungen eine Beeinträchtigung des öffentlichen oder wirtschaftlichen Lebens wahrscheinlich.

In den letzten Jahren ist die Anzahl der gemeldeten Sicherheitsvorfälle expotentiell angestiegen. Ebenso ist zu verzeichnen, dass die Schadenswirkung durch kriminelle Handlungen (u.a. Phishing, Betrug, Erpressung) stark ansteigt. Auch die Warnungen hinsichtlich terroristischer Attacken sind nicht unbegründet. Das IT-Sicherheitsmanagement ist heute in einer extrem schwierigen Situation. Der Zeitraum zwischen der Anzeige einer Schwachstelle und dem Eintritt einer Schadenswirkung wird immer geringer und läßt kaum noch Zeit für umfangreiche Analysen und vorbeugende Maßnahmen.

Die Skizzierung der Bedrohungssituation macht deutlich, dass Sicherheitsteams und CERTs neue Arbeitsweisen und Methoden entwickeln müssen, um dieser Situation letztendlich nicht nur reaktiv, sondern weiterhin auch proaktiv begegnen zu können. Ein vom deutschen CERT-Verbund vorangetriebener gemeinschaftlicher Ansatz ist das Projekt CarmentiS - Zeitnahe Information über neue Sicherheitslagen im deutschen Internet.

2 IT-Frühwarnung

In den letzten 12 Monaten hat der Begriff „Frühwarnung“ im Bereich IT-Sicherheit eine Inflation erlebt; inzwischen werden sowohl Alarmierungssysteme – bei denen es nur um die rasche Information einer bestimmten Zielgruppe geht – als auch Forschungsarbeiten mit diesem publikumswirksamen Begriff in Zusammenhang gebracht. Dabei ist das zunehmende Interesse der Politik und Wirtschaft hierfür mit verantwortlich, da diese endlich die existierende Lücke erkannt haben und Lösungen einfordern.

Die Analogien, die für Frühwarnung jedoch oftmals bemüht werden, greifen auf Warnungen vor Naturkatastrophen zurück und fordern letztlich etwas – nicht nur für den Bereich der Computernetzwerke – technisch Unmögliches, nämlich das Verhalten von Menschen vorherzusagen. Bei Kenntnis neuer Sicherheitslücken kann mit einer fast 100%-iger Wahrscheinlichkeit davon ausgegangen werden, dass ein neuer IT-Angriff erfolgt. Dies kann daher nicht der alleinige Maßstab sein, die Kernfragen sind anderes: Wann wird ein Schadprogramm das erste Mal eingesetzt? Wo wird es eingesetzt? Wird es in einem Wurm zu finden sein? Wird man einen solchen Angriff automatisiert erkennen können?

Trotz dieser ernüchternden Worte gibt es natürlich Verfahren, um Angriffe so wie früh wie möglich zu erfassen. Es ist jedoch unabdingbar, Frühwarnung sinnvoll zu definieren, um seriös über die technischen Möglichkeiten zu diskutieren. Nach unserer Auffassung muss ein Kompromiß zwischen Schnelligkeit und Genauigkeit gefunden werden:

Aufgrund eindeutiger Erkenntnisse, die noch möglichst wenige betreffen, sind Informationen zu verteilen, die vielen (noch nicht Betroffenen) helfen, und (insgesamt) Schlimmeres vermeiden!

3 Der Kern eines IT-Frühwarnsystems

Ziel der in diesem Projekt engagierten CERTs ist es, mit überschaubaren Mitteln in einem definierten Zeitraum Verbesserungen zu schaffen, die tatsächlich einen ersten Schritt hin zu einer besseren Frühwarnung darstellen und einen Rahmen bereitstellen, um sich der Vision einer „Frühwarnung“ substantiell zu nähern.

Da gerade CERTs möglichst frühe Vorab-Informationen benötigen, gibt es dort schon länger Ansätze, schnell und automatisiert neue Trends zu erkennen und auf Angriffe zu reagieren. Nun gilt es, die aus verschiedenen Quellen stammenden Daten zusammenzuführen und zur Erstellung von Lagebildern bezüglich aktueller Bedrohungen zur Verfügung zu stellen, zum Beispiel für Trendanalysen und vergleichende statistische Auswertungen.

Entgegen den Vorurteilen einer Reihe von Experten kann ein Projekt mit dem Titel „Frühwarnung“ nicht primär ein Sensorennetz sein. Stattdessen muss es vielmehr die Verknüpfung von menschlicher und (teil-)automatisierter Informationsverarbeitung darstellen, um alle Aspekte abdecken zu können. Bei der Analyse neuer Sicherheitslücken müssen aufkommende Informationen über Angriffe im Netzwerk und Metainformationen genutzt werden. Entsprechend der aufgestellten Hypothesen ist dann gezielt nach neuen Angriffsignaturen zu suchen. Grundlage für die Analyse stellt zunächst die enge Kooperation zwischen den verschiedenen Teams im CERT-Verbund dar, die durch die Schaffung einer kooperativen Arbeitsumgebung verstärkt wird. Durch diese Umgebung werden die dezentralen Sicherheitsexperten zu einem virtuellen Kompetenzzentrum zusammengefaßt, in dem zukünftig auch Experten anderer Fachbereiche interdisziplinäre zusammenarbeiten werden.

Alle gesammelten, angereicherten und aufbereiteten Informationen müssen durch geeignete Schnittstellen, die durchaus einheitlich angelegt werden sollen, aber dennoch unterschiedliche Sichten unterstützen müssen, Nutzern zugänglich gemacht werden. Zunächst werden hier vier Nutzergruppen identifiziert:

- Operative Stellen auf nationaler Ebene, deren Interessen vor allem in Informationen zum Thema Lagebild und zur Verbesserung des Krisenmanagements liegt,
- Betreiber kritischer Infrastrukturen erhalten ein aktuelles Lagebild, das sie in die Lage versetzt, geeignete vorbeugende Maßnahmen zu ergreifen, sobald sich akute Gefahren abzeichnen,
- CERT-Teams, deren Interessen vor allem in der Betreuung der jeweils eigenen Zielgruppe, deren Alarmierung und der Aufklärung von Angriffen auf IT-Systeme der Zielgruppe liegt,
- Partnern, die zu den Zielen des Projekts beitragen, z. B. durch die Bereitstellung und Sammlung von Informationen oder Daten über Sensoren, und zumindest Zugriff auf einen Teil der bereitgestellten Informationen in Form von Fallstudien und Einzelberichte hat.

Auf Grundlage dieser Basisinfrastruktur als Kern eines IT-Frühwarnsystems wird einerseits kurzfristig die Versorgung mit zeitnahen Informationen verbessert werden, andererseits steht eine Plattform für die weitergehende Erprobung verfügbarer Ansätze und Entwicklung neuer Strategien zur noch rascheren Erkennung zur Verfügung.

4 Erfolgsfaktoren

Das Projekt CarmentiS ist ein konsequenter Schritt des deutschen CERT-Verbundes, die im Code-of-Conduct[1] aufgeführten Ziele zu erreichen. In Zusammenarbeit mit der öffentlichen Hand wird ein wichtiger Beitrag zum Schutz nationaler Netze der Informationstechnik und zur schnellen Reaktion bei auftretenden Sicherheitsvorkommnissen geleistet.

Ein erfolgreicher Ausbau einer Basisinfrastruktur, hin zu einen nationalen IT-Frühwarnsystem wird wesentlich davon abhängen, ob die Faktoren, die bislang die Arbeit des CERT-Verbunds geprägt und letztendlich dieses Projekt erst ermöglicht haben, auch auf eine größere Anzahl von Organisationen übertragen werden kann. Ohne die Bereitschaft aller Beteiligten, sich auf die Einhaltung und Umsetzung der folgend genannten Faktoren zu verständigen, ist ein nationales IT-Frühwarnsystem nicht umzusetzen.

- Informationsaustausch
- Bereitstellung von Ressourcen
- Unterstützung von Standards
- Vertrauen und Schutz der Betroffenen

Das Projekt ist offen für andere, denn nur durch die Beteiligung vieler Organisationen kann ein umfassender Einblick in die Realität unserer heutigen Netze und Anwendungen gewonnen werden. Wichtiger Teilaspekt des Projekts ist daher die Entwicklung geeigneter Kooperationsmodelle, um eine Beteiligung weiterer Organisationen zu ermöglichen, sowie die Ausarbeitung einer Basis, durch die auch andere die gewonnenen Informationen und Mehrwerte nutzen können, wobei jedoch die zu fordernden Grundsätze eingehalten werden müssen.

5 Ausblick

Mit dem Projekt CarmentiS[2] haben sich Partner aus dem deutschen CERT-Verbund entschlossen, zusammen mit der öffentlichen Hand eine Basisinfrastruktur für die weitergehende Erprobung verfügbarer Ansätze und Strategien zur noch rascheren Warnung bis hin zur Frühwarnung zu schaffen. Im Hinblick auf die heute unzureichende Versorgung mit zeitnahen Informationen wird hierbei bereits kurzfristig eine Nutzung des Piloten für die operativen Tätigkeiten der verschiedenen CERTs und Sicherheitsorganisationen vorgesehen und damit potentiell Betroffene konkret warnen und vor Schäden bewahren.

[1] Deutscher CERT-Verbund, Code of Conduct, www.cert-verbund.de
[2] Der Projektstart war im November 2005.