DuD
Datenschutz und Datensicherheit

IDS – Vision und Wirklichkeit

Warum Intrusion Detection Systeme gescheitert sind

Dirk Fox

Vision

Mitte der 90er Jahre des vergangenen Jahrhunderts brachen Intrusion Detection Systeme (IDS) aus den Elfenbeintürmen der Hochschullabors. Zahlreiche Hersteller, darunter Anbieter von Netzkomponenten wie Cisco, Spezialisten für Kommunikations-Sicherheitslösungen wie NAI, aber auch Experten für das Netzsicherheitsmanagement wie BindView und Firewall-Anbieter, z. B. Axent, erweiterten ihre Produktpalette um Intrusion Detection Systeme oder -Funktionen. Die Idee eines IDS war bestechend: Statt des unablässigen Kampfs gegen die Windmühlen ständig neuer Angriffsmethoden und entdeckter Schwachstellen versprachen sie die Erkennung und Alarmierung bei Anomalien im Netz, die auf einen Angriff hindeuten könnten – durch Live-Beobachtung und Analyse des gesamten Netzverkehrs. So könnten vor allem auch bis dahin unbekannte Angriffe erkannt werden, so die Erwartung.

Zahlreiche Systeme boten ergänzende Funktionen, wie das Einspielen von Sicherheitspatches auf kritischen Systemen oder die Zusammenführung und zentrale Auswertung („single point of control“) von Logfiles der Sicherheitssysteme (Firewall) oder sogar die Überwachung von Policy-Verstößen durch die IT-Nutzer.

Weg also mit der ständigen Unsicherheit, dass die eingesetzten IT-Systeme unbekannte Sicherheitslöcher in den Anwendungen oder Betriebssystemen besitzen könnten, die ein Angreifer möglicherweise bereits missbraucht. Weg mit dem Dauerstress des permanenten Einspielens neuer (oft ungetesteter) Patches – im Vertrauen auf das IDS zu Gunsten eines langsameren, aber systematischen Patch-Managements. Und weg mit der Befürchtung, dass ein unerkannter Trojaner auf einem internen System lauern und bereits aktiv sabotieren könnte.

Wirklichkeit

Tatsächlich sah die Realität der Systeme erheblich nüchterner aus – die Mühen der Ebene kamen zurück. Nicht nur, dass die Konfiguration und Bedienbarkeit der Systeme sehr komplex waren und erhebliches Know-how voraussetzten. Das Kernproblem lag in der Natur der Sache: Will man „Anomalien“ erkennen, setzt das voraus, dass sich „normales“ von „nicht normalem“ Kommunikationsverhalten unterscheiden lässt. Und genau hier liegt das systematische Problem eines IDS:

- Das beobachtbare Kommunikationsverhalten in einem Netz unterliegt starken „Schwankungen“, die sich von Anomalien praktisch nicht unterscheiden lassen und daher in erheblichem Ausmaß Fehlalarme auslösen.
- Viele Angriffe (z.B. Trojaner) haben ein Kommunikationsverhalten, das die Alarmierungsschwelle nicht überschreitet, da es vom „normalen“ Verhalten des Systems nicht unterschieden werden kann.
- Auffällige Angriffe hingegen, wie z.B. Denial-of-Service-Attacken, werden zwar detektiert. Allerdings betreffen sie auch das IDS, sodass eine Alarmierung nur über einen getrennten Kanal gelingt – und in der Regel überflüssig ist, denn einen solchen Verfügbarkeitsangriff bemerkt man auch ohne IDS.

Die Antwort auf diese Ernüchterung waren „Signatur“-basierte Systeme, die ähnlich Virenscannern nach Verhaltensmustern bekannter Angriffssysteme suchten. Allein: Dies war die Absage an das eigentliche Ziel eines IDS, unbekannte Angriffe zu detektieren. Den aus bekannten Angriffen resultierenden Bedrohungen ließ sich mit weniger Aufwand und wirkungsvoller durch ein systematisches Patch-Management begegnen.

Zahlreiche IDS-Projekte in Unternehmen scheiterten in den vergangenen Jahren an den Aufwänden für Installation, Konfiguration und vor allem den Betrieb. Hohe Investitionen verstauben in der Ecke, seit die Verantwortlichen erleben mussten, wie Fehlalarme die (ohnehin zunehmend knappen) personellen Ressourcen des IT-Bereichs binden – ohne einen erkennbaren Sicherheitsgewinn.

Folgerungen

Das Thema IDS ist inzwischen von der Wunschliste der Unternehmen verschwunden; viele Installationen wieder deaktiviert. Überlebt haben nur wenige „Randfunktionen“ eines IDS, wie

- die Zusammenführung und Analyse von Logfiles z.B. zur Vorfallsbearbeitung im Rahmen forensischer Analysen, die inzwischen in Sicherheitsmanagement-Konsolen aufgegangen sind;
- automatisierte Patch-Management-Lösungen, die ähnlich IDS-Produkten das Netz nach eingesetzten IT-Systemen abscannen und die Patch-Stände identifizieren;
- Reporting-Funktionen, die einen Überblick über die Zahl der abgewehrten und möglicherweise auch erfolgreichen Angriffe durch Schadsoftware liefern.

Der Idee eines IDS könnte allerdings in anderer Form doch noch eine Zukunft beschieden sein – als Honeypot. Denn unter einer Bedingung lassen sich Netzanomalien leicht erkennen: Wenn ein System beobachtet wird, das nicht genutzt wird. Jede Aktivität auf einer solchen „Köder“-Maschine deutet auf einen erfolgreichen Angriff hin – der auch weitere Systeme im Netz betreffen kann. Mit den dabei gewonnenen Erkenntnissen kann man dann gezielt suchen – und spart sich, ganz nebenbei, die Sammlung von Terabytes personenbezogener Daten. Datensparsamkeit ganz konkret.