

Frühwarnsystem gegen Cyber-Angriffe

Mit Anomalieerkennung zum Ziel

Der erfolgreiche Angriff auf das Playstation Network von Sony hat wieder einmal gezeigt, wie leicht es für einen Angreifer ist, in ein Unternehmensnetzwerk einzubrechen. Vor allem aber, welche Folgen ein solcher Angriff haben kann. Das aktuelle Beispiel belegt die Notwendigkeit für „Frühwarnsysteme“ gegen Cyber-Angriffe auf große Unternehmensnetze. Ein Forschungs- und Entwicklungsprojekt an der Hochschule Fulda hat sich die Ausarbeitung geeigneter Techniken und die Entwicklung einer produktreifen Lösung zum Ziel gesetzt.

Unternehmen öffnen heute ihre IT-Systeme, um Partnern und Kunden Services aus ihrem Intranet heraus (E-Commerce und E-Business) zur Verfügung stellen zu können. Dabei nimmt die so genannte Deperimetrisierung der Netzstrukturen zu: Geschäftsprozesse verteilen sich auf mehrere Unternehmen, und Dienstleistungen werden über das Internet erbracht (Cloud Computing, Service-orientierte Architekturen). So verwundert es nicht, dass in den

vergangenen Jahren besonders Angriffsszenarien auf Unternehmensnetzwerke und kritische Infrastrukturen aus dem Cyberspace – wie E-Threats, Wirtschaftsspionage oder terroristische Angriffe – zugenommen haben. IT-Sicherheit muss daher inhärenter Bestandteil der gesamten IT-Infrastruktur sein („Ubiquitous IT Security“). Trotz verschiedener Sicherheitstechniken, wie Firewall-Systeme, Malware-Filter und

Access-Control-Lösungen, nutzen Angreifer immer wieder Schwachstellen in Protokollen und Softwareprodukten aus, um unautorisierten Zugriff auf Rechnersysteme zu erlangen. Die Weiterentwicklung der Intrusion-Detection-Systeme (IDS) steht daher schon längst auf der Agenda mehrerer Forschungsaktivitäten. So verfolgt etwa die Hochschule Fulda in Zusammenarbeit mit dem Fuldaer ITK-Spezialisten Nethinks und weiteren Unternehmen aus Hessen die Entwicklung eines neuartigen Frühwarnsystems, um auch bisher unbekannte Angriffe – wie „Zero Day“- und „Less Than Zero Day“-Angriffe – zu erkennen.

Der Ansatz ist dabei, die Informationen aus klassischen Netzwerk-Monitoring- und Analyse-Tools mit den Informationen aus Sicherheitsanwendungen zu verknüpfen. Klassische Monitoring- und Analyse-Tools zur Kontrolle und Überwachung komplexer heterogener Netzwerktopologien können Störungen in Netzkomponenten und Endsystemen schnell lokalisieren und ihre Ursachen beheben, verfügen aber meist über keinerlei Funktionen zur effektiven Erkennung und Abwehr von Angriffsszenarien auf unternehmensweite Rechnernetze.

In dem dreijährigen, vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Vorhaben ist vorgesehen, zusammen mit den Kooperationspartnern das Monitoring-Werkzeug Monet zu dem Monitoring- und Security-Werkzeug Secmonet auszubauen. Monet ist dabei eine Distribution verschiedener Open Source Tools für das Netzwerk-Management. Darin enthalten sind unter anderem das Monitoring-Tool Open-NMS, das Netzwerkanalyse-Werkzeug Netflow sowie die IP-Adressverwaltung IP-Plan.

Dafür wurden zunächst Vorgehensweisen und Methoden verfügbarer Open Source als auch kommerzieller Produkte zur Angriffs- und Schwachstellenerkennung (Intrusion-Detection-/Prevention-Systeme, Penetration Testing, Anti-Malware und andere) auf ihre Anwendbarkeit in Monet untersucht und geeignet weiterentwickelt. Weiterhin lassen sich die aus den klassischen Netzwerk-Management-Anwendun-

gen (wie Open-NMS, Netflow und IP-Plan) zahlreich vorhandenen Informationen in den Bereichen Fehler-, Konfigurations-, Leistungs- und Adress-Management zur Angriffserkennung heranziehen. Da die Struktur der Daten sehr unterschiedlich ist, sind diese in ein einheitliches Datenmodell zu transferieren (Features und Attributes), um alle gewonnenen Informationen ganzheitlich auswerten zu können.

Intrusion-Detection-Systeme lassen sich üblicherweise in „Misuse Detection“ und „Anomaly Detection“ klassifizieren. Während Misuse-Systeme eine Datenbank mit Mustern (Signatures) bereits analysierter Angriffe verwenden, um aktuelle Eindringversuche festzustellen, klassifizieren anomaliebasierende Systeme Abweichungen im Netzwerk von einem als „normal“ erkannten Zustand als anomales Verhalten und deuten damit auf Real-time-Angriffsversuche hin. Der Vorteil der Anomaly Detection besteht in der Erkennung auch bisher unbekannter Eindringversuche.

Um die „False Positive“-Rate der Angriffsmeldungen möglichst gering halten zu können, sind allerdings noch einige Herausforderungen zu bewältigen. Dazu gehören unter anderem die Selektion der Features mit dem meisten Informationsgehalt hinsichtlich der Beschreibung des Netzwerkzustands, das Erkennen von Abhängigkeiten zwischen den Features und deren geeignete Gruppierung (Feature Reduction Techniques), die Auswahl sinnvoller Schwellenwerte zur Klassifizierung der Anomalien und die Beschreibung des-

sen, was als normales Netzwerkverhalten („Normal Behavior“) anzusehen ist. Techniken (Classifier), die das Netzwerkverhalten als normal oder anomal beurteilen, existieren ebenfalls zahlreich und besitzen jeweils Vor- und Nachteile. Das Forschungsprojekt untersucht derzeit so genannte „Unsupervised Machine Learning“-Methoden. Mit der Implementierung eines „Self-Organizing Map“-Algorithmus besteht die Hoffnung, eine effektive Klassifizierung des Netzwerkzustands und des Angriffstyps zu erhalten. Häufig unterschiedene Angriffskategorien zur Beschreibung eines anomalen Netzwerkverhaltens sind Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L) sowie Probe. Aufbauend darauf ist vorgesehen, auch Funktionsweisen und Schadwirkung verschiedener Malware-Arten und deren Infektionswege zu eruierten, Schwachstellen SOA-basierender (Service-orientierte Architektur) Infrastrukturen zu analysieren und Angriffsszenarien in derartigen Netzstrukturen aufzudecken, um schließlich innovative Ansätze für effektive Schutzmechanismen entwickeln zu können.

Professor Dr. Hans-Ulrich Bühler und Michael Batz/pt

Professor Dr. Hans-Ulrich Bühler hat seit 1990 eine Professur für Angewandte Mathematik im Fachbereich Angewandte Informatik der Hochschule Fulda inne und begleitet das Forschungsprojekt federführend.

Michael Batz begleitet stellvertretend für Nethinks das Hochschulforschungsprojekt.

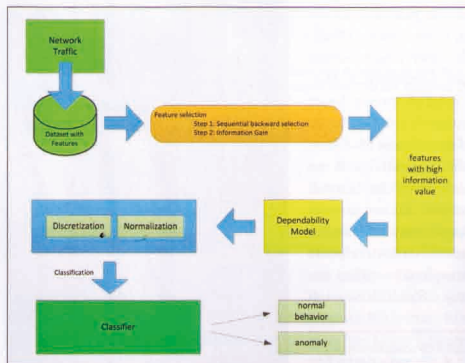
Angriffskategorien

Grundlegend lassen sich Angriffe auf Netzwerke in verschiedene Kategorien einteilen: Denial of Service: Bei einer DoS-Attacke versucht ein Angreifer, die Ressourcen eines Systems so zu binden, dass dieses nicht mehr fähig ist, legitime Anfragen zu behandeln.

User to Root: Bei einer U2R-Attacke besitzt ein Angreifer zunächst einen Nutzer-Account auf einem System. Diesen hat er möglicherweise durch Sniffing, „Brute Force“-Angriffe oder Social Engineering erhalten. Von diesem Benutzer-Account aus ist es ihm möglich, mittels eines Exploits, Root-Rechte zu erlangen.

Remote to Local: Ein Angreifer kann bei R2L zunächst ein System nur über das Netzwerk erreichen und einzelne Datenpakete an die Maschine senden, besitzt aber keinen Nutzer-Account. Mittels eines Exploits erhält er Zugriff auf das System – genau wie ein lokaler Nutzer.

Probe: Durch Probing-Attacken versucht ein Angreifer, Informationen über ein Computernetzwerk oder ein lokales System zu erhalten. Port Scans fallen zum Beispiel in diese Kategorie.



Schematische Darstellung der Anomalieerkennung im Forschungsprojekt Secmonet an der Hochschule Fulda.

...BLEIBEN SIE FLEXIBEL. MIT KOMMUNIKATIONS-LÖSUNGEN, DIE IHR WACHSTUM BERÜCKSICHTIGEN.



Wer das Morgen gestalten will, muss heute damit beginnen.

bintec WLAN Controller: Die ideale Wireless Kommunikationslösung für Mittelstand, Dienstleister und Freiberufler.



Funkwerk bietet Ihnen mit dem innovativen bintec WLAN Controller die Möglichkeit, leistungsstarke Wireless Netzwerke einfach, schnell und ohne Spezialkenntnisse zu konfigurieren und zu managen. Der WLAN Controller automatisiert administrative Arbeiten, ermöglicht den reibungslosen Betrieb von WLAN Infrastrukturen und eignet sich für VoWLAN Telefonie – „Voice Ready“. Das sichert Ihnen bereits heute einen Vorsprung, kombiniert mit hohem Investitionsschutz. Unsere ganzheitlichen Lösungen haben alle ein Ziel: Ihre Kommunikation so einfach und sicher wie möglich zu gestalten.

Optimieren Sie die Wettbewerbsfähigkeit Ihres Unternehmens mit einer maßgeschneiderten, professionellen Business-Kommunikationslösung von Funkwerk!

SPRACHE, DATEN, SICHERHEIT.

funkwerk
enterprise communications

Funkwerk Enterprise Communications GmbH
Südwestpark 74
D-91044 Nürnberg
Tel. +49-911-9673-0
www.funkwerk-ec.com