FACTA UNIVERSITATIS (NIŠ)
SER.: ELEC. ENERG. vol. 15 Dec. 2002, 341-347

Ein Sicherheitsverbund als zusätzlicher Schutz für das lokale Netzwerk

Thomas Droste

Abstract: Der hier vorgestellte Sicherheitsverbund nutzt freie Ressourcen und führt eine dezentrale Datenaufnahme und Analyse durch. Dabei wird eine Komponentenstruktur genutzt, die einzelne Aufgaben zusammenfasst und auf jedem Rechner bereitstellt. Der Sicherheitsverbund arbeitet parallel zu bestehenden Sicherheitsmechanismen und unterstützt diese durch die zusätzliche und unabhängige Sicherheitsfunktion. Neben einer Vorstellung des Sicherheitsverbundes aus [4] wird auf Funknetzwerke und die resultierenden Besonderheiten im Sicherheitsverbund eingegangen.

Keywords: Rechnerverbund,verteilte Ressourcenutzung, Firewall, WLAN, VPN.

1 Einleitung

Die Forderung nach Sicherheit in vernetzten (kabelgebundenen und kabellosen) Systemen stellt ständig neue Anforderungen an Sicherheitsmechanismen. Als klassisches System kontrolliert eine Firewall den Datenfluss am Übergangspunkt vom Teilnetzwerk bzw. lokalen Netzwerk (LAN) zum übergeordnetem Netzwerk (LAN bzw. WAN). Weitere installierte Schutzmechanismen (z.B. Intrusion Detection Systeme, IDS) im eigenen Netzwerk untersuchen den Datenstrom bis zu einem Koppelpunkt. Sicherheitsverletzungen und Penetrationen innerhalb eines Netzwerkes können folglich erkannt werden. Eine interne Sicherung über das gesamte LAN hinweg ist schwer möglich. Der interne Datenverkehr kann nur begrenzt überprüft werden, wobei alle Systeme zusätzliche Hardware benötigen. Die Einbindung

Manuscript received September 19, 2002
Der Author ist am Lehrstuhl für Datenverarbeitung, Ruhr-Universität Bochum, 44780 Bochum, (e-mail: droste@etdv.ruhr-uni-bochum.de).

sekundärer Netzwerkschnittstellen, so z.B. eine WLAN-Karte in einem Notebook, ist analog zu einem nicht erlaubten Einwahlpunkt früherer Sicherheitsbetrachtungen und den damit verbundenen Risiken schwer zu erkennen und zu handhaben. Auch diese Anbindung wird durch den Sicherheitsverbund erkannt und überwacht.

1.1 Definition eines Sicherheitsverbundes

Ein Sicherheitsverbund fasst ein verteiltes Sicherheitssystem, das auf allen Rechnern im lokalen Netzwerk aufgesetzt und in Funktion ist, zusammen. Dieser netzwerkweite Betrieb gewährleistet, dass alle Rechner gemeinsam als ein Sicherheitssystem interagieren können. Ein zusätzliches Serversystem, wie z.B. für eine zentrale Firewall, wird nicht benötigt, da der Einsatz auf den einzelnen, vorhandenen und genutzten Arbeitsplatzrechnern erfolgt.

Agieren mehreren Rechnern zusammen, d.h. stehen diese in einer speziellen Beziehung zueinander bzw. verfolgen ein gemeinsames Ziel (z.B. die Lösung einer Rechenaufgabe), so symbolisieren diese einen Rechnerverbund. Diese Beziehung bzw. das Ziel der Zusammenarbeit ist zunächst unabhängig von einem Sicherheitsverbund.

Eine Migration von einem Rechnerbund bzw. mehreren Rechnerverbunden zu einem Sicherheitsverbund findet statt, wenn die einzelnen Rechner Teil eines verteilten Sicherheitssystems sind. Ein Sicherheitsmanagement beschreibt die notwendige Interaktion innerhalb des Sicherheitsverbundes und koordiniert Funktionen zwischen den einzelnen Rechnern und Rechnerverbunden.

1.2 Ziel des Sicherheitsverbundes

Das Ziel des Sicherheitsverbundes ist es, den Datenstrom im gesamten lokalen Netzwerk aufzunehmen, lokal und verteilt zu überprüfen sowie reagierend einzugreifen [1][2]. Das Konzept des Sicherheitsverbundes setzt auf eine heterogene Struktur im Netzwerk auf und agiert parallel zu bestehenden Sicherheitsmechanismen. Der aufzubauende Sicherheitsverbund - und damit der Aufbau einer geschtzten Zone im lokalen Netzwerk - nutzt die vorhandenen Ressourcen (Rechner und freie Prozessorzeit) optimiert und agiert transparent für einen lokalen Benutzer. Eine redundante Akquisition der Netzwerkdaten ermöglicht eine Analyse und Nachforderung von verfügbaren Mitschnitten aus verschiedenen Quellen. Eine weitere Besonderheit ist die Unabhängigkeit von einem zentralen System. Jeder Rechner kann einen

Sicherheitsverbund autark aufbauen und alle erreichbaren Rechner integrieren. Einzelne Komponenten auf jedem System übernehmen die Aufgabe zur Erkennung des Sicherheitsverbundes, der Datenakquisition, der lokalen und verteilten Analyse, der Reaktion auf eine Sicherheitsverletzung sowie der Kommunikation zur Interaktion zwischen den einzelnen Komponenten (als Multi-Client/Server-Dienst). Über das Netzwerk sollen gleiche Komponenten miteinander interagieren und Informationen an andere Komponenten weiterleiten.

1.3 Funktionsgruppen

Der Aufbau des Sicherheitsverbundes erfolgt durch die Erkennung aller Rechner im lokalen Netzwerk über alle Teilnetzwerke gesammelt [5]. Ein zugehöriger Rechner (mit aktiven Komponenten des Sicherheitsverbundes) wird als Mitglied eingebunden. Alle übrigen Rechner (z.B. neu installierte oder fremde Rechner) werden von der Kommunikation ausgeschlossen. Alle Mitglieder zusammen bilden folglich den Sicherheitsverbund. Jedes Mitglied des Sicherheitsverbundes ist allen Rechnern bekannt und steht zur Kommunikation im Sicherheitsverbund bereit. Auf Basis der ermittelten Rechner wird eine redundante Datenaufnahme zugeordnet. Dabei kennt ein Rechner nur die zu überwachenden und nicht die ihn überwachenden Rechner.

Die Akquisition der Netzwerkdaten erfolgt von jedem Rechner im Sicherheitsverbund unabhängig und wird lokal zwischengespeichert. Eine Reduzierung das Datenvolumens der zu überwachenden Rechnern erfolgt durch Filterung.

Die lokale (zeitnahe) Analyse der zwischengespeicherten Daten findet nach einer netzwerkweiten Regelbasis des Sicherheitsverbundes statt. Eine Analyse erfolgt durch Filter, die auf jedes einzelne Paket angewendet werden. Nicht nur der rechnerspezifische Datenverkehr, sondern auch der Datenverkehr von redundant zu überwachenden Systemen wird analysiert. Ein Mitglied im Sicherheitsverbund kann bei Erkennung einer Sicherheitsverletzung direkt auf den betroffenen Rechner zugreifen und das Einzelsystem und durch Mitteilung an andere Mitglieder im Sicherheitsverbund das Gesamtsystem schützen.

Die Zusammenführung aller aufgenommenen Netzwerkmitschnitte zu einem netzwerkweiten Datenmitschnitt ist Voraussetzung fr die weitere Analyse. Alle Rechner im Sicherheitsverbund werden für eine verteilte Analyse (für z.B. zeitgedehnte Vorgänge) miteinbezogen. Es wird eine Bewertung

aller Rechner für eine Analyseaufgabe (inkl. Datenvolumen) durchgeführt und die benötigte Zeit zur Bearbeitung abgeschätzt (Nutzung als Cluster). Bei einer bekannten Sicherheitsverletzung erfolgt eine direkte Reaktion vom analysierenden Rechner aus. Jede Analyse wird einmalig verteilt und während der Abarbeitung nicht zwischen Rechnern transferiert. Lediglich das Ergebnis wird zurückgeliefert.

Reaktionen des Sicherheitsverbundes auf eine Sicherheitsverletzung sind z.B. die Aussendung einer Benachrichtigung an den Netzwerkverwalter oder ein aktive Steuerung des betroffenen System (Blockierung von Verbindungen, Verbindungsabbau, Abmelden eines Benutzers, Herunterfahren eines Systems, etc.).

Die Kommunikationskomponente regelt sämtlichen Datenverkehr sowie die Benachrichtigungen und kann Komprimierungsmechanismen enthalten. Eine Sicherung sämtlicher Kommunikation wird durch Verschlüsselung erzielt, weiterhin ist eine Authentifizierung der einzelnen Rechner im Sicherheitsverbund notwendig.

2 Erkennungsvorgang im lokalen Netzwerk

Die Erkennung identifiziert alle Rechner im lokalen Netzwerk und integriert diese in den Sicherheitsverbund. Als Ergebnis werden die ermittelten Rechnerparameter in einer Liste auf jedem Rechner im Sicherheitsverbund geführt.

Der Sicherheitsverbund muss seine Mitglieder kennen, um diese in den Verbund integrieren zu können. Dabei kann ein Rechner entweder Mitglied des Sicherheitsverbundes sein oder nicht dem Sicherheitsverbund zugehören.

Der erste Fall stellt den etablierten Sicherheitsverbund dar, d.h. auf jedem kontaktierten Rechner läuft eine Instanz der Komponente zur Erkennung. Ein Rechner ist dann Teilnehmer des Sicherheitsverbundes und folglich erreichbar, wenn die Komponente installiert und der Rechner eingeschaltet ist. Ist ein Rechner ausgeschaltete, zählt dieser nicht zum aktiven Sicherheitsverbund und ist kein aktiver Teilnehmer. Er wird jedoch als passives Mitglied klassifiziert.

Der zweite Fall umfasst die Gruppe von Rechnern, die nicht Mitglieder des Sicherheitsverbundes sind. Auf diesen Systemen sind keine Komponenten des Sicherheitsverbundes aktiv. Entweder ist ein Rechner neu (noch nicht administriert und konfiguriert) in das lokale Netzwerk eingebunden worden oder es handelt sich um einen fremden (nicht unter den administrativen

Bereich des lokalen Netzwerkes fallenden) Rechner. Letztere Möglichkeit ist von besonderer Bedeutung, da dies ein Eindringen in die Netzinfrastruktur bedeutet und erkannt werden muss. Insbesondere in Bezug auf Funknetzwerke ist diese Möglichkeit besonders kritisch. Im Gegensatz zu einer festen Ankopplung an einen speziellen Netzwerkanschluss (Netzwerkdose) ist eine Verbindung z.B. an ein Zugangspunkt (Access Point, AP) ohne direkten (räumlichen) Zugang über die Luftschnittstelle möglich.

2.1 Betrachtung von Wireless LAN (WLAN)

Ein Funknetzwerk (WLAN) ist für ein mobiles Rechnersystem durchaus praktisch, birgt jedoch durch die nicht abgekapselte Umgebung und feste Netzwerkverdrahtung Risiken.

Bei der Sicherung dieser mobilen Geräte, wie z.B. Notebooks und PDAs, ist ein rechnerbasierter Schutz unumgänglich, der mit netzinternen Kontrollinstanzen interagieren muss. Eine Integrierung mobiler Systeme in andere Netzwerke ist durch den Einsatz von AP unproblematisch. Der Sicherheitsverbund kann neu integrierte Rechner automatisch erkennen und die Kommunikation restriktieren. Erste Kontrollinstanz bei WLAN-APs sind die SSID und eine einstellbare (WEP-)Verschlüsselung, wodurch ein freier Zugang (z.B. über SSID="ANY") nicht mehr möglich ist. Dies bietet den Vorteil, dass nur mit bekannten Einstellungen der Zugang erlaubt ist. Zusätzlich hierzu kann jetzt über die Erkennung das mobile System als Mitglied im Rechnerverbund identifiziert werden. Insbesondere bei "ad-hoc"-Netzwerken ist ein Schutz durch den Sicherheitsverbund möglich. Hierbei können die Geräte auch miteinander kommunizieren und benötigen keine WLAN-Koppelelement zum übrigen LAN. Die Gefahr besteht in der unbekannten Nutzung von WLAN-Elementen ohne Infrastruktur. Durch den Sicherheitsverbund werden diese mehrfachen Netzwerkverbindungen über andere Schnittstellen zum LAN erkannt und können restriktiert werden. Wird bei einer WLAN-Infrastruktur ein Router benutzt, der mobile Systeme versorgt, so ist durch den Sicherheitsverbund eine Integrierung des WLAN möglich. Hierbei ist jedoch keine Adressumsetzung mittels NAT zwischen beiden Netzwerken (LAN/WLAN) erforderlich. Um eine gefahrlose Integrierung von mobilen Geräten in das eigene lokale Netzwerk und damit in den Sicherheitsverbund durchzuführen, ist der Aufbau einer VPN-Verbindung zum eigenen lokalen Netzwerk erforderlich. Ein Rechner ist dann über eine eigene lokale Adresse eingebunden, wobei dieser wiederum authentifiziert ist. Die Anbindung des über ein VPN konnektierten Rechners wird automatisch bestimmt, wodurch

Analysen innerhalb des leistungsfähigeren LAN bleiben (z.B. WLAN: 11 MBit/s, LAN: 100 MBit/s).

Eine Entkopplung von mehrerer VPNs (WLAN, externe Zugänge über das Internet) ist sinnvoll, da alle Verbindungen über einen Netzwerkkoppelrechner (zumeist eine Firewall) laufen und dort analysiert werden.

Diese Sicherheitsbetrachtungen gelten für jegliche Luftschnittstellen (WLAN, Infrarot, Bluetooth, etc.), wodurch die Mobilität und Flexibilität eingeschränkt wird. Sind bei heutigen Geräten Funkschnittstellen zumeist nicht integriert, kann sich dies jedoch schnell ändern, analog zu eingebauten Modems und Ethernet-Netzwerkschnittstellen.

2.2 Einschränkungen beim Erkennungsvorgang

Ein Rechensystem, das nicht aktiv Pakete aussendet bzw. auf Pakete antwortet, kann nicht ber den Erkennungsvorgang erkannt werden. Da es sich um eine Softwareumsetzung handelt, werden physikalische Änderungen am Netzwerkmedium (Einstecken eines Netzwerkkabels) nur von Koppelelementen erfasst. Ein Switch kann einen Link zu einer Netzwerkschnittstelle erkennen, fr ein Drittsystem am gleichen Switch (aber anderem Port) ist die Erkennung unmöglich.

Bei einer WLAN-Verbindung ist ebenfalls nur der kontaktierte AP über einen weiteren Kommunikationspartner informiert, wobei bei Funksignalen eine einseitige Verbindung (nur Empfang) zum Auswerten von Daten ausreicht. Somit ist bei einem Funknetzwerk eine unerlaubte Verbindung (bei entsprechender Konfiguration des Endsystems), ohne die Möglichkeit, diese zu erkennen, möglich.

Die Nutzung von Verschlsselung und Authentifizierung ist der einzige Weg, damit nicht erkennbare Systeme auch weiterhin von der Kommunikation ausgeschlossen bleiben [3].

3 Zusammenfassung

Gerade der Einsatz von mobilen Endgeräten und drahtloser Netzwerkanbindung haben gezeigt, dass ein Sicherheitssystem mehr als aus nur einigen zentral im Netzwerk angeordneten Mechanismen bestehen muss. Jedes Endsystem - insbesondere Notebooks - sind leicht mit einer WLAN-Karte auszustatten und zu betreiben. Folglich ist ein Sicherheitssystem auf jedem Rechner im lokalen Netzwerk (LAN, WLAN) zwingend notwendig, wobei

eine netzwerkübergreifende Sicherung als gemeinsames Schutzsystem anzustreben ist. Wird ein mobiles Gerät in ein anderes Netzwerk transportiert, darf es nicht automatisch integriert werden. Dies gilt für eigene (Mitglieder des Sicherheitsverbundes) und für fremde (Gäste, etc.) Nutzer mit mobilem Endgerät.

References

[1] T. Droste: *Sicherheitsdienste in einem Rechnerverbund.* In Horster, Patrick: Kommunikationssicherheit im Zeichen des Internet, S. 1-12, Vieweg & Sohn, Braunschweig, 2001.

[2] T. Droste, A. Ruhl: *Aufgaben bei verteilter Datenakquisition und dessen Zusammenführung fr die Analyse.* In Horster, Patrick: Enterprise Security, S. 155-164, IT-Verlag für Informationstechnik GmbH, Höhenkirchen 2002.

[3] T. Droste, M. Vogel: *Richtlinien fr eine verteilte Sicherheitsinfrastruktur.* In Horster, Patrick: Enterprise Security, S. 100-110, IT-Verlag für Informationstechnik GmbH, Höhenkirchen 2002.

[4] T. Droste: *Konzept eines komponentenbasierten, verteilten Sicherheitsverbundes*, Dissertation, Fakultät für Elektrotechnik und Informationstechnik, Ruhr-Universität Bochum, Bochum 2002.

[5] V. Schüppel: *Entwicklung einer Client-/Server-Applikation zum Informationsaustausch von Systemdaten zwischen entfernten Systemen*, Diplomarbeit D341, Lehrstuhl für Datenverarbeitung, Ruhr-Universität Bochum, Bochum 1999. Ein Sicherheitsverbund als zusätzlicher Schutz für das lokale Netzwerk