Gefahren-Abwehr mittels LAN-Analyse

Eine Übersicht.

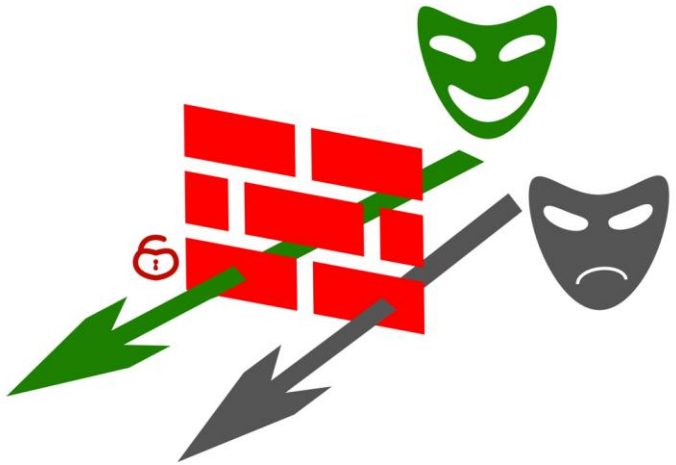
VORTRAG:

FRANK R. WALTHER

SYNAPSE NETWORKS GMBH

WWW.SYNALYST.NET

Sind Sie (sich) wirklich sicher?



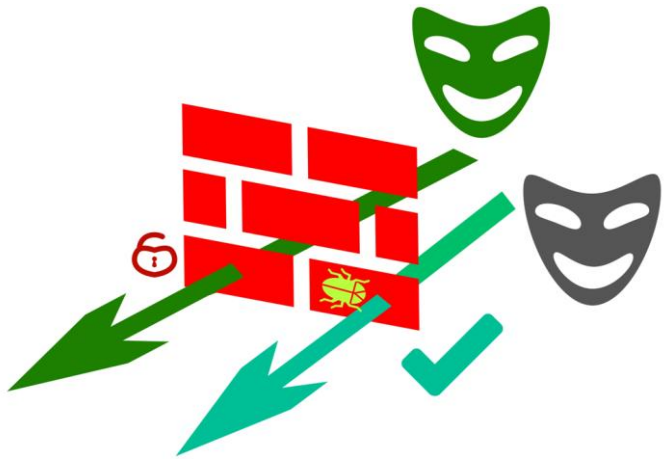
Sie haben eine Firewall ?

Die Firewall blockt Eindringlinge

Doch was ist, wenn die Firewall versagt ?

LAN-Analyse sichert Sie ab vor Überraschungen

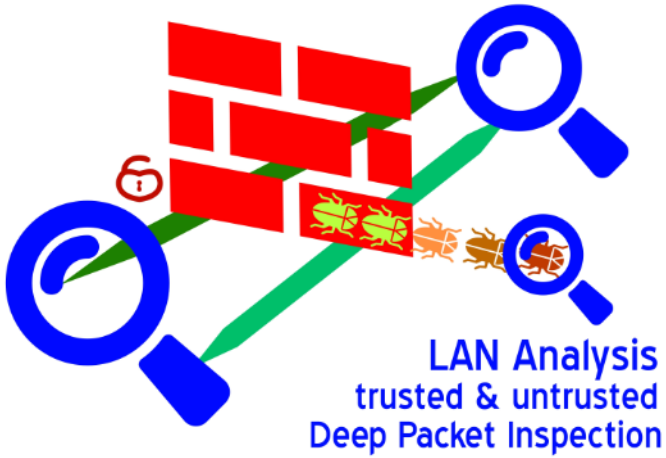
Was, wenn die Firewall durch einen Bug das Tor für ungebetene Besucher still geöffnet hat - und niemand das bemerkt, bevor es zu spät ist ?



Wissen Sie wirklich, was Ihre Firewall durchlässt ?

Die Firewall selbst kann das ggf. nicht erkennen.
Sie denkt, dass sie genau tut, wie befohlen.

LAN-Analyse



- LAN-Analyse "drinnen" wie "draußen" untersucht genau die Datenströme und verifiziert die Firewall.
- Sollte die Firewall ein Leck haben, durch Bug oder Konfiguration, wird es erkannt.

Keine LAN-Analyse = keine Sicherheit!

Motivation(en) zur LAN-Analyse

- Betriebsbereitschaft erhöhen
  Ausfallrisiko mindern
  Migrationsfähigkeit bewahren/schaffen
- Betriebskosten vermindern
  Personaleinsatz vermindern
  Reaktionszeiten verkürzen
- Datenschutz/-sicherheit erhöhen
  Datenabfluss verhindern
  Angriffsflächen so klein halten wie möglich
- Forensik / Nachweisfähigkeit bei Vorfällen
  Bewahrung der aufgezeichneten LAN-Daten
  zur Erbringung gerichtsfester Beweise
- Bereitstellung von Fakten
  Beschaffung von Planungsgrundlagen
  Leistungskontrolle externer Dienstleister

Allgemein übliche IT-Schutzfunktionen (Auswahl)

- Perimeter-Schutz: Erkennung und Abwehr von Angriffen an der Außengrenze:
  Firewall, Web-Proxy, Mail-Server
- Innerer Schutz: Erkennung und Abwehr von Angriffen und Eindringlingen innen: IDS, AntiVir, Security-Agenten auf Clients/Servern
- Zugriffs-Schutz:
  Autorisierung, Authentisierung
  Benutzer-Konten, -Passworte, -Rechte
- Daten-Verschlüsselung
  Verschlüsselung auf Festplatten-Ebene
  Verschlüsselung auf Datei-Ebene
- Big-Data-Analyse: Durchforsten von E-Mails, Chats, Zugriffs-Protokollen, um Hinweise auf Untreue, Korruption etc. zu erhalten

Echtzeit-Instanzen (Firewalls etc.): Beschränkungen

- Im Moment des Geschehens wird das Ereignis erkannt und gemeldet; aktiver Eingriff durch Blocken von Vorgängen; (relativ) schnell eingerüstet & betriebsfertig
- Einzelne Aktionen/Ereignisse werden erkannt, Zusammenhänge zwischen zeitlich und räumlich verteilten Ereignissen eher weniger
- Gespeichert werden die Protokolle (log files), die Original-Daten eher weniger oder gar nicht (auch Frage der Preisklasse)
- Ggf wird erst durch Aggregieren von Syslog-Meldungen in SIEM-Systemen der Blick auf Zusammenhänge frei

Client/Server Software-Agenten: Beschränkungen

- Im Moment des Geschehens wird das Ereignis erkannt und gemeldet; aktiver Eingriff durch Blocken von Vorgängen; ggf. flächendeckende Echtzeit-Überwachung
- Konsequent eingesetzt, gehören die Agenten auf alle (möglichst viele) Endgeräte (Clients, Server, Mobile Devices, etc.) -> ggf. teuer (Zahl der Lizenzen), ggf. wartungsintensiv; langjährige Bindung an einen Lieferanten
- Planung & Pilot ggf. problematisch, da Beweis der Wirksamkeit nur im Produktions-Netz möglich und da die Einrüstung eines Test-Piloten ggf. selbst eine Perimeter-Verletzung darstellt und entsprechende Genehmigungen verlangt. Entfernung der Agenten nach Test auf Produktionsgeräten könnte problematisch sein, da ggf. nicht rückstandsfrei entfernbar

LAN-Analyse: Vorteile und Möglichkeiten

- Auf Grund geringer Kosten können viele Subnetze mit LAN-Analyse ausgestattet werden: verteilte Analyse weltweit möglich
- Da über sog. Mirror Ports gearbeitet wird, ist das Verfahren non-invasiv und stellt keine Perimeter-Verletzung dar; Planung+Pilot problemlos jederzeit & preiswert möglich
- Einfache Technik, preiswert, sofort einrüstbar, sofort mit wertigen Ergebnissen; Bewahrung der Original-Daten (Ring Buffer);
  Online-Analyse möglich (Echtzeit/Nahzeit);
  Offline-Analyse möglich (Forensik)
- Software-Lösungen: langsamer als Echtzeit-Instanzen, daher ggf nicht für Core-Backbones geeignet, sondern für einzelne Client/Server-Subnetze

Datenschutz, Persönlichkeitsrechte, DSGVO

Sofern über das Betriebs-LAN/WAN keine persönlichen Daten versendet werden, handelt es sich bei den Daten sämtlich um **Betriebsdaten**, die dem Unternehmen gehören und nicht dem Mitarbeiter. Analyse darf alles sehen, was nicht die Schutzrechte von Mitarbeitern oder Dritten verletzt.

Personenbezogene Daten, die nicht ohne Einwilligung der Betroffenen in der Analyse als solche erfasst und verarbeitet werden dürfen (Auswahl): LAN-Verkehr der Personalabteilung; VoIP-Telefonate; private E-Mails von Mitarbeitern (sofern betrieblich zugelassen); etc. -

Diese Daten werden daher grundsätzlich von der Analyse ausgeschlossen, sofern kein Rechtfertigungsgrund und keine richterliche Anordnung vorliegen.

Regelungen: Betriebsvereinbarung; betrieblicher Datenschutz(beauftragter)

DSGVO: regelt die Überlassung, Übertragung, Speicherung, automatische Verarbeitung persönlicher Daten. - Genau das tut LAN-Analyse nicht.
Daher ist die DSGVO im Regelfall auf die LAN-Analyse **nicht anwendbar**.

Wireshark - tcpdump - libpcap

- Wireshark bzw. tcpdump sind inzwischen die Standard-Werkzeuge für das Aufzeichnen und Sichten von LAN-Aufzeichnungen (capture files, trace files). Das verwendete libpcap-Format ist inzwischen quasi-universell und eignet sich daher bestens für die Aufzeichnung

- Die Analyse der aufgezeichneten Daten durch Wireshark selbst ist jedoch starken Einschränkungen unterworfen, ist unvollständig und oft sogar fehlerhaft

- Es können problemlos Erweiterungen "oben drüber" gesetzt werden, die von den Treibern der Wireshark-Suite aufgezeichnete Daten analysieren

- Mit diesen (als Wireshark-Erweiterung wirkenden) Experten-Systemen lassen sich weltweit verteilte Netzwerke in Nahzeit analysieren und in SIEM-Systeme integrieren

Weltweite Analyse verteilter LAN/WAN-Netze

Mittels Aufzeichnung des Datenverkehrs durch die Treiber der Wireshark-Suite (bzw durch tcpdump) im libpcap-Format sowie mittels Analyse dieser Daten durch ergänzende Experten-Systeme lassen sich problemlos weltweit arbeitende Netzwerke überwachen

Die Einbindung in vorhandene SIEM-Systeme ist möglich, was zusätzliche Möglichkeiten der Daten-Aggregation und -Analyse schafft. Auf diese Weise kann LAN-Analyse mit vorhandenen IT-Sicherheits-Strukturen zusammen arbeiten

SIEM: Security Information & Event Management

Je größer die verwendeten Datenspeicher sind (Festplatten), um so länger sind die gespeicherten Zeitfenster (ring buffer). Dies können Tage, Woche, Monate sein (je nach Subnetz).

SIEM, LogFiles & Forensik

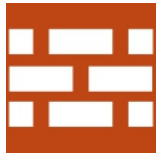
Wenn eine einzelne aktive Komponente (Firewall, Server, IDS, etc) oder das zentrale SIEM-System Alarm schlägt, hat es entweder ein einzelnes Ereignis erkannt oder eine Kette zusammenhängender Ereignisse - aber immer nur auf Grund höchst begrenzter Sichtweite und Meldungen

Diese Alarm-Meldungen können zutreffend sein - oder so nebulös wie der Blick in die berühmt-berüchtigte Glaskugel im vorletzten Wohnwagen hinter dem Zirkuszelt

LAN-Analyse kann der Forensik an dieser Stelle helfen: Durch die Aufzeichnung des LAN-Verkehrs kann bei SIEM-Alarm bzw bei Verdacht auf einen Sicherheits-Vorfall (oder auf eine technische Störung) der beteiligte Datenverkehr nachträglich isoliert und analysiert werden.

LAN-Analyse mit intelligenten Filtern erlaubt es, auch aus riesigen Datenmengen (GB,TB) genau *die* LAN-Pakete heraus zu holen, mit denen sich Vorfälle aufklären lassen

Firewall: (un)trusted black box



Firewalls sind unverzichtbarer Baustein der IT-Sicherheits-Stuktur. Nur: Wie kann das Unternehmen sicher sein, dass die Firewall auch tut, wofür sie bezahlt wird ?

Was, wenn ein Bug oder eine Fehl-Konfiguration dazu führen, dass die Tür weit offen steht - anstatt geschlossen zu sein ? Ohne, dass es jemand merkt ?

Nur die LAN-Analyse des eingehenden und ausgehenden Datenverkehrs einer Firewall, sowohl auf der "trusted" wie auch der "untrusted" Seite, kann wirklich die Sicherheit geben, dass die Firewall auch tatsächlich "dicht hält".

Praxis-Beispiel: *Nach Einrüstung der brandneuen Firewall stellte die LAN-Analyse fest, dass die neue Firewall (im Gegensatz zur alten) interne Daten nach außen abfließen ließ. Es stellte sich heraus: Die Firewall-Entwickler hatten versehentlich in der Bediener-Oberfläche die Beschriftungen "open"/"blocking" vertauscht. Wer "blocking" anklickte, stellte - ohne es zu wissen - im Hintergrund auf "open".*

LAN-Analyse: Querschnittsaufgabe

Jedes Unternehmen leidet (oder droht, zu leiden) unter mangelnder Koordination und Kooperation zwischen den verschiedenen Abteilungen und Lieferanten/Gewerken.

Wie sollen Fehler gefunden werden, bei denen die Geräte/Maschinen und Gewerke verschiedenster Abteilungen und Lieferanten beteiligt sind - durch Menschen, deren mangelndes Zusammenwirken die Fehler überhaupt erst ermöglicht bzw bewirkt hat ?

LAN-Analyse blickt weiter, über alle Grenzen von Abteilungen, Gewerken und Lieferanten hinaus.

LAN-Analyse erkennt Beziehungen, Abläufe und Wirkungsketten, die sonst entweder verborgen blieben - oder nur mit z.T. absurd großem Aufwand ermittelbar wären

LAN-Analyse = niedrigere IT-Kosten, mehr Effizienz

LAN-Analyse als Querschnittsdienst kennt keine Grenzen - nicht von Abteilungen, Gewerken oder Lieferanten.

Statt Schuldzuweisungen und/oder blindem Herumstochern im Heuhaufen gibt es mit wenig Aufwand schnelle, klare Fakten

Statt bei Fehlern unbekannter Wirkungsform alle Abteilungen und Lieferanten blind zu beauftragen ("macht mal, aber schnell") ("viel hilft viel"), ist es sinnvoller, erst einmal durch LAN-Analyse den Fehler und die beteiligten Maschinen zu isolieren, um dann klare Arbeitsaufträge zu verteilen: an die wenigen, die es angeht

Das spart Personaleinsatz.
Das spart **Zeit**.

Das vermindert Kosten.
Das spart **Geld**.

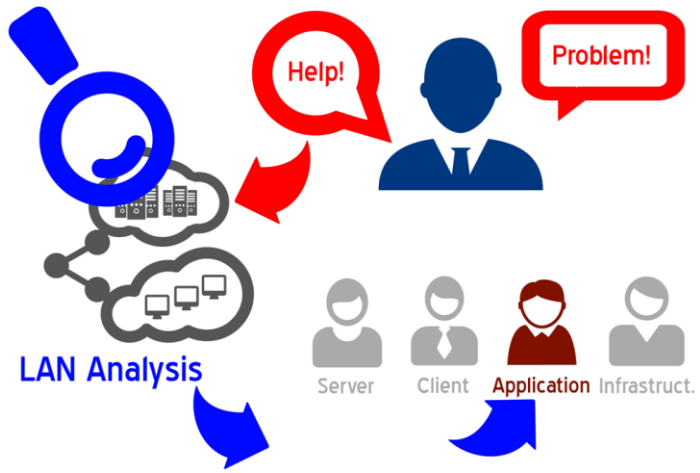
Troubletickets: Multitasking

Das Multi-Tasking-System:

Es kommt eine völlig unbestimmte Anwender-Klage. Niemand weiß etwas Genaues. Der Auftrag geht an alle Abteilungen gleichzeitig.

Die Admins und Techniker **aller** Abteilungen sollen gleichzeitig ohne genaue Angaben den Fehler suchen. **Zeit und Resourcen werden verschwendet.**

Troubletickets: Singletasking



Das Single-Tasking-System:

Der Auftrag geht zunächst an die LAN-Analyse.

Dort wird erkannt, ob es ein Problem ist von: Server, Client, Application, Comm./Infrastructure.

Erst dann wird der Auftrag weiter gegeben in die Fachabteilung: **keine Zeit wird verschwendet.**

LAN-Analyse: liefert Dokumentation

Automatische Analyse erzeugt umfangreiche IT-Inventarisierung:

Listen aller MAC-Adressen, IP-Adressen, NetBIOS/WINS/DNS-Namen, Domains & Forests, Server-Shares, KERBEROS-Realms, Subnetze, Router, etc etc: unverzichtbares Material für die IT

Die Erfahrung lehrt: Wer hier auf die Daten der Fachabteilungen wartet, kann lange warten. Das ist nicht akzeptabel.

Analyse-Agenten sammeln diese Daten automatisch:

Wo steht welches Gerät, mit welchen Adressen, Namen, Diensten, Anwendungen ? - Das ermöglicht zudem **Sicherheits-Analysen**.

Durch Soll-Ist-Abgleich kann regelmäßig ermittelt werden, ob im Netzwerk wirklich **genau die** - **und nur die** - Komponenten arbeiten (Hardware/Software), die geplant und gewollt sind.

LAN-Analyse: durch wen ? und wie ?

Nur **sicherheitsüberprüftes** bzw zweifelsfrei vertrauenswürdiges und **loyales Personal** sollte LAN-Analyse betreiben

Damit ist **ausgeschlossen**, dass z.B. ein IT-Generalunternehmer (GU), der als Externer die IT betreibt, auch die LAN-Analyse durchführt: es darf nicht sein, dass ein Dienstleister sich selbst überwacht (Zielkonflikt, **Loyalitätskonflikt**)

Es kann vorteilhaft sein, einen vom GU getrennten und wirtschaftlich nicht verbundenen Spezial-Dienstleister zu beauftragen

Die Analyse mag ein Externer durchführen. Die Daten aber bleiben immer intern. Das Personal hat Fernzugriff - aber nur für die Videodaten (RDP), nicht für Datei-Übertragung. LAN-Daten dürfen nicht nach außen abfließen (sofern nicht wirklich gewollt)

LAN-Analyse: unverzichtbar & lohnend zugleich

Es konnte gezeigt werden:

LAN-Analyse lässt sich schnell und einfach einrüsten
LAN-Analyse hilft, die Betriebsabläufe zu verbessern
LAN-Analyse vermindert ggf spürbar den Personal-Einsatz
LAN-Analyse ist ohne Probleme bzgl DSGVO/Datenschutz möglich

LAN-Analyse kann proaktiv eingesetzt werden
LAN-Analyse kann reaktiv eingesetzt werden (Forensik)
LAN-Analyse hilft, die potenziellen Angriffsflächen klein zu halten

LAN-Analyse kann Beweise liefern (gerichtsfeste zudem), wo sonstige Systeme (Firewalls, IDS, SIEM, etc) zwar Meldung machen, aber den tatsächlichen Hergang nicht voll sichtbar machen (können)

Es gibt also <u>keinen</u> Grund, LAN-Analyse <u>nicht</u> einzusetzen.

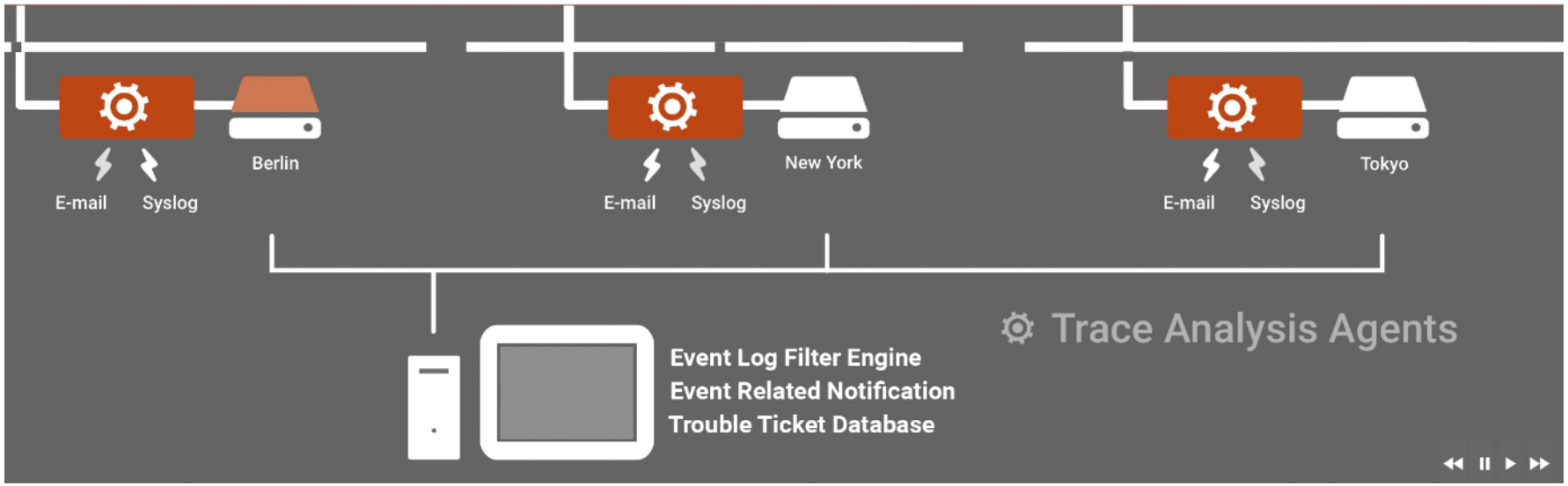
Impressum

Synapse Networks GmbH
Peter-Bischof-Str. 2A
55435 Gau-Algesheim

fon: 06725-9990710
fax: 03212-7962773

Geschäftsführer:
Frank R. Walther
f.walther@synapse.de

Kunden-Betreuung:
Ceren Bakir
c.bakir_team@synapse.de



www.synalyst.net