synalyst

smart network analysis

Kurze Darstellung der LAN-WAN-Analyse
mittels Deep Packet Inspection und Syslog-SIEM

Software – Managed Service - Strategie

Synapse Networks GmbH

≡ Übersicht ≡

Inhaltsverzeichnis

Einführung

Ausgangslage im Umfeld IT-getriebener Unternehmen

Überall rüsten Unternehmen auf im Umfeld von IT-Security, z.T. mit Managed Services.

Dabei wird ersichtlich Wert gelegt auf umfassende Angebote, die möglichst viele Bereiche abdecken, in denen Sicherheit von Bedeutung ist, darunter der Betrieb von Firewall, Zugangsverwaltung, Session Management – und vor allem mit: Security Information and Event Management (SIEM).

In diese Bemühungen passt ein spezieller Dienst, der LAN-Analyse in Form von Deep Packet Inspection betreibt: Datenpakete und Datenflüsse werden daraufhin untersucht, ob technische Fehler, Konfigurationsprobleme oder Gefahren für Sicherheit und Integrität vorhanden sind.

Viele der üblichen Melde-Systeme sind rein reaktiv, da sie nur bereits aufgetretene Ereignisse erfassen.

Die Ergänzung wäre, nicht nur nach dem zu suchen, was bereits geschieht, sondern auch nach dem, was künftig geschehen könnte – indem aus dem Hintergrundrauschen diejenigen Signale heraus gefiltert werden, aus denen sich die Fehler und Gefahren der Zukunft ableiten lassen; und indem genau die Fehler erkannt werden, die von anderen Schutz-Komponenten und von SIEM nicht gesehen werden (können).

Siehe unten: Beispiele aus der Praxis – Gefährliche Fehler, die kein SIEM je zu sehen bekam – die aber synalyst meldete.

Mit der synalyst Software-Suite kann dies erreicht werden.

Schnell und niederschwellig: Bedarfs-Ermittlung und Leistungsnachweis ohne großen Aufwand

Vom ersten Interesse bis zur Vorführung oder Test-Piloten stehen bei vielen Systemen hohe Hürden, großer Aufwand, langwierige Planungen und Genehmigungsverfahren – schon allein deswegen, weil kein Unternehmen gerne Dritt-Anbieter mit aktiven Komponenten nur-mal-eben-so ins eigene Netzwerk lässt.

synalyst Analyse hat dieses Problem nicht, da non-invasiv gearbeitet wird, über uni-direktionale Mirror-Ports (Analyse lediglich einer Kopie des Datenverkehrs, ohne direkten Kontakt mit ihm). Mit weniger als einer halben Stunde Vorbereitungszeit kann vor Ort und live und real vorgeführt werden - bei gleichzeitig vernachlässigenswertem Einsatz an Personal, Zeit, Mitteln.

Ein System, das zur IT-Sicherheit beitragen soll, muss nicht nur Leistungsfähigkeit zeigen, sondern auch Effizienz und Niederschwelligkeit in ihren technischen und organisatorischen Voraussetzungen.

Die synalyst Analyse benötigt für einen ersten wirkungsvollen Einsatz vor Ort ohne Vorplanung lediglich:

1 Netzwerk-Admin (Mirror-Port schalten, Patch-Kabel legen)
1 Switch-Mirror-Port
1 Laptop mit der synalyst Analyse-Software
1 Beamer im Besprechungsraum
1 Vormittag/Nachmittag für die Live-Analyse und/oder für die Sichtung der Analyse-Ergebnisse

Die Erfahrung zeigt: Mehr Aufwand braucht es nicht, um zu überzeugen, ...

- dass im Netzwerk Dinge zu sehen sind, die dort nicht sein sollten;
- dass die Analyse-Technik schnell, umfassend und verständlich klare Ergebnisse liefert.

Mit geringstmöglichem Aufwand und in kurzer Zeit wird schon beim Erst-Aufbau vor Ort und live der Nachweis erbracht, dass Bedarf besteht, und dass der Bedarf gedeckt werden kann.

synalyst Analyse bietet ein operatives Optimum: minimaler Aufwand, maximales Ergebnis.

Nutzen im Tages-Betrieb: Managed Service

Die Ergebnisse der synalyst Analyse ...

- helfen, Mann-Tage zu sparen, und die Effizienz des IT-Betriebs steigern;
- helfen, den Mittel-Einsatz zu steuern, indem weniger auf Verdacht, sondern präzise zielgenau nach Fehlern gesucht wird und diese sodann punktgenau abgestellt werden – beispielsweise dadurch, dass klare Arbeitsaufträge exakt an die zuständigen Admins und Techniker vergeben werden (und nicht, wie oft zu beobachten, an mehrere gleichzeitig, weil die Struktur eines Fehler-Geschehens nicht klar ist bzw nicht eindeutig den Zuständigkeiten zugeordnet werden kann).

Automatisierte Dauer-Analyse erzeugt ständig Befunde, die in klare Arbeitsaufträge umwandelt werden.

Dieser Ansatz führt zu Kosten-Ersparnissen sowie höherer Betriebsbereitschaft bzw Verfügbarkeit.

synalyst Analyse ist also kein ideologie-getriebenes "nice to have", sondern erforderliches Betriebsmittel.

IT-Sicherheit in kleinen und mittleren Unternehmen (KMU)

- vielerorts viel zu teuer

Viele der am Markt propagierten Systeme zu Analyse, Monitoring, Anomalie-Erkennung, SIEM etc leiden unter mindestens einem der folgenden Nachteile:

- Sie sind schon im Anschaffungspreis für KMU zu teuer
- Sie sind im Betrieb viel zu teuer / haben zu hohe TCO (Total Cost of Ownership)
- Verlangen schon für einen ersten Test-Aufbau einen viel zu großen, kaum leistbaren Aufwand

- viel zu oft überfordernd

Schon in der Vorbereitung eines Test-Piloten scheitern oft die Projekte oder werden unangenehm hinaus gezögert, weil ...

- das Unternehmen die erforderliche Personal-Freistellung nicht leisten kann
- die einzurüstende Technik zuvor Sicherheits-Freigaben braucht, die Aufwand mit sich bringen, weil
- die Sicherheits-Protokolle zur Einrüstung aktiver Komponenten beachtet werden müssen
- die vorhandenen Komponenten (Server, Router, Switches, etc) ggf neu konfiguriert werden müssen, damit sie ihre Syslog-Meldungen an das neue SIEM-Center senden (das kann Hunderte von Komponenten treffen, um am Ende aussagefähige Ergebnisse zu bringen)

- verlangt sofortige Einsatzfähigkeit: niederschwellig, voraussetzungslos einrüstbar

IT-Sicherheit kann nur geschaffen werden, wenn sie möglichst schnell nutzbare Ergebnisse liefert, ohne dass die Organisationsfähigkeit des Unternehmens überlastet bzw beeinträchtigt wird. **synalyst** Analyse verlangt im Kern nur den Mirror-Port am Switch/Router, dessen Datenverkehr überwacht werden soll.

IT-Sicherheit ist gegen die Regeln der Wirtschaftlichkeit nicht möglich

- Personalverfügbarkeit

Sowohl die Vorbereitung (Projektierung, Test-Pilot, etc) als auch der spätere Betrieb ergeben aus Sicht insbesondere von KMU nur Sinn, wenn sie das vorhandene Personal nicht belasten und die laufenden Aufgaben nicht vernachlässigt werden.

Damit ein neues System zur Schaffung oder Erhöhung der IT-Sicherheit nicht auf Ebene der Organisation bzw der Betriebsabläufe selbst zum Sicherheitsrisiko wird, darf sie keine unerfüllbaren Forderungen an die Personalverfügbarkeit stellen.

- Skalierbarkeit

Wenn schon der Einstieg in ein System zu Analyse, Monitoring, Anomalie-Erkennung, SIEM etc hohe fünf- bis sechsstellige Beträge und zwei- bis dreistellige Manntag-Kontingente verlangt bzw verbraucht, ist es vermutlich nicht nur zu teuer, sondern auch zu immobil, was seine Anpassungsfähigkeit angeht.

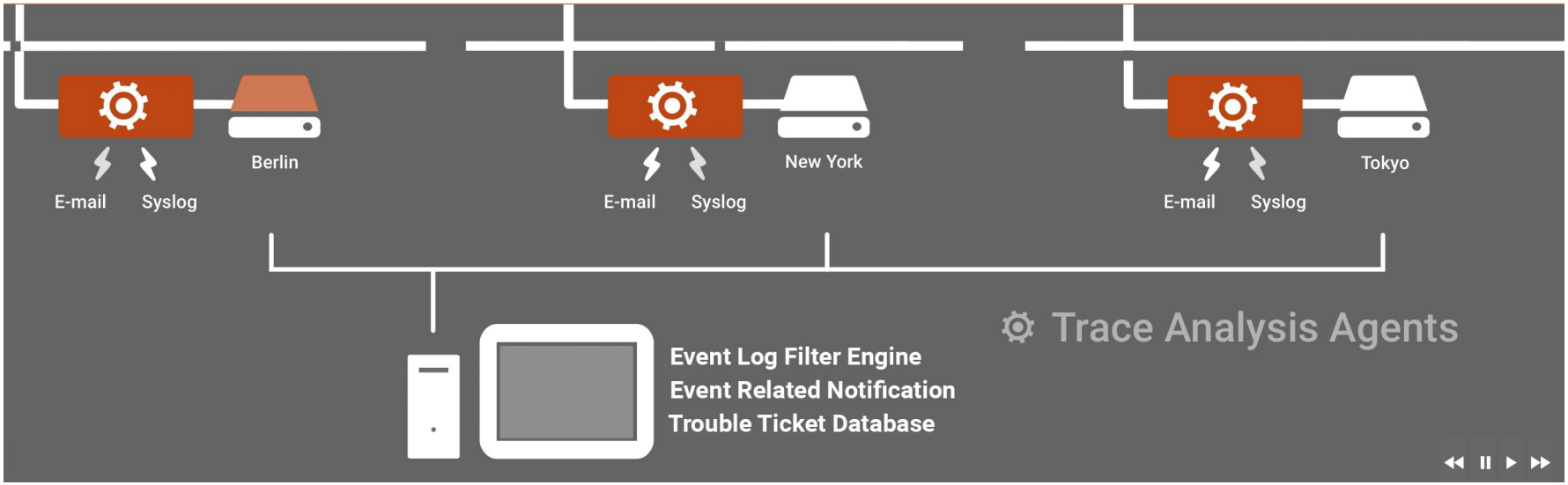
Wirtschaftlich und organisatorisch "stemmbar" ist es dann – und nur dann - , wenn es mit geringstem Aufwand und sofort ad-hoc in Betrieb genommen werden kann.

- Schneller Einstieg, beherrschbare Kosten, sofort nutzbare Ergebnisse

synalyst Analyse bietet das, was KMU brauchen: die unkomplizierte, mit weniger als 1 Manntag machbare Einrüstung und Inbetriebnahme bei gleichzeitig unvergleichlich niedrigen Kosten, und das alles mit umfassenden, sofort nutzbaren Ergebnissen.

synalyst Analyse eignet sich daher auch zum mobilen und/oder einmaligen Einsatz (z.B. Schnell-Audits).

Weltweite Analyse mit synalyst-Agenten: 20 Mio Events täglich, 400 Event-Filter (SIEM)



Animierte Darstellung der verteilten Netzwerk-Analyse:

www.synalyst.net

Ein von **Synapse Networks GmbH** betreuter Kunde hat weltweit 25-30 **synalyst** Analyse-Agenten im Einsatz, die täglich durchschnittlich ca 20 Mio Ereignis-Meldungen via Syslog an den zentralen Syslog-Sammler schicken. Die dortige Event Log Filter Engine enthält mehrere Hundert Ereignis-Filter in der Filter-Bibliothek; diese werden auf die per Syslog eingegangenen und gesammelten Event-Log-Meldungen anwendet (SIEM). Auf diese Art werden die gemeldeten Ereignisse sortiert, priorisiert, archiviert und in Berichten zugänglich macht.

synapse & synalyst

synalyst bezeichnet sämtliche Elemente der von Synapse Networks GmbH erbrachten Managed Services zur Analyse von LAN-WAN-Datenkommunikation, in Sonderheit die damit verbundene Software-Suite samt der zugehörigen Dienstleistungen.

Mit der **synalyst** Suite wird der LAN-Datenverkehr aufgezeichnet, semi-archiviert, analysiert, bewertet.

Die Semi-Archivierung der LAN-Pakete im sog. Ring Buffer umfasst – je nach Hardware-Ausstattung, Datendurchsatz und Einstellung – Tage, Wochen, Monate und schafft dadurch die Voraussetzungen zu Forensischer Analyse, indem bei Bedarf der binäre Datenstrom im Rückgriff aufs Archiv zur Verfügung steht.

Firewall, Intruder Detection System, Server Log etc sowie die mit Meldungen aus dieser Quelle gefüllten SIEM-Systeme zeigen nur das, was anderswo erkannt und wie-auch-immer gedeutet und gewichtet wurde.

Das ist viel – und doch zu wenig. Sowohl reaktive Forensik wie auch proaktive Analyse können den letzten, bei Bedarf auch gerichtsfesten Beweis nur liefern, wenn die in Rede stehenden Ereignisse nicht nur mit nachgelagerten Meldungen von Dritt-Systemen, sondern auch mittels der originalen Datenpakete nachvollzogen und offen gelegt werden können.

Die Schaffung und Wahrung von Sicherheit im Sinne von Betriebsverfügbarkeit (Abwesenheit von Störungen) und Datenvertraulichkeit (Abwesenheit von Fremdzugriffen und Datenabflüssen) verlangt die permanente Analyse mit Experten-Systemen sowie die permanente Durchmusterung der Ergebnisse mit bedarfsaktuellen Ereignis-Filtern.

Der **synalyst** Managed Service von Synapse Networks GmbH liefert genau das.

Software & Service

Synapse liefert für die dauerhafte, automatisierte Experten-Analyse die Software und die Dienstleistung.

Software: Aufzeichnung und Auswertung der LAN-Pakete, Erzeugen von Event Log und Berichten; Aktualisierung der Analyse-Software (jeweils neuester Stand).

Service: Sichtung der Ergebnisse; Betrieb einer Troubleticket-Datenbank; Nachverfolgen aller Arbeiten zum Beheben erkannter Fehler und Sicherheitsgefahren; Beratung des Kunden.
Je nach Vertrag sind auch Rufbereitschaft und definierte Reaktionszeiten möglich.

Troubleticket-Datenbank

Die von Synapse gepflegte Troubleticket-Datenbank ist der hauptsächliche Übergabe-Punkt der Analyse-Leistung - und somit das, was der Kunde im Ergebnis zu sehen wünscht: eine klare Handlungsanweisung.

Über die Troubleticket-Datenbank (z.B. MS-Sharepoint) werden die Arbeitsaufträge an die Admins und die Techniker vergeben und ggf eskaliert. Sobald es im jeweiligen Troubleticket eine Antwort des zuständigen Bearbeiters gibt, verifiziert Synapse den Erfolg der Arbeiten, indem die Analyse den Beweis dafür liefert, ob (bzw dass) das beanstandete Verhalten tatsächlich beseitigt ist – oder eben nicht.

SIEM – Ergänzung und Integration

synalyst arbeitet intensiv mit Event-Log-Meldungen via Syslog; sie werden gefiltert, sortiert, priorisiert.

Technische Ansätze werden allgemein zusammen gefasst unter der Bezeichnung:

SIEM Security Information and Event Management

synalyst Analyse arbeitet innerhalb der eigenen, abgeschlossenen Software-Suite SIEM-ähnlich; andererseits kann die synalyst Analyse die eigenen Event-Meldungen in vorhandene SIEM-Systeme einspeisen.

synalyst Analyse kann ohne Kopplung an SIEM-Systeme völlig unabhängig und eigenständig arbeiten, kann aber auch ergänzend in SIEM-Systeme integriert werden. Üblich ist, dass vorhandene SIEM-Systeme zwar stark "gefüttert" werden mit Meldungen aktiver Komponenten (Clients, Server, Router, Firewalls, etc), seltener aber von Netzwerk-Analyse-Systemen auf Ebene der LAN-Pakete (Deep Packet Inspection).

synalyst Analyse sieht sich daher nicht nicht im direkten Wettbewerb mit anderen Systemen.

Empfängt ein SIEM-System Event-Meldungen der synalyst Analyse, kann – in Abhängigkeit zur Speicher-Kapazität im Ring Buffer der ⚙ Analyse-Agenten (s.u.) – auf die originalen Binär-Daten bzw LAN-Pakete zwecks Beweissicherung zurück gegriffen werden – was wiederum unerlässliche Voraussetzung ist für forensische Analyse. Dies ist z.B. bei Incident-Meldungen von Firewalls nicht selbstverständlich.

synalyst Analyse erkennt und meldet Fehler, auch schwerste, die Standard-SIEM nicht sichtbar macht.

Siehe hierzu die "Beispiele aus der Praxis" (nächste Seite).

Wireshark – starkes Werkzeug, ergänzungsbedürftig: synalyst verkürzt den Zeit-Einsatz

synalyst arbeitet mit seinem Modul MintMagic ...

- entweder mit Einzel-Lizenz als Stand-Alone-Analyzer -oder- im Verbund vieler ⚙ Analyse-Agenten, die dezentral im Unternehmensnetz verteilt sind und die den Datenverkehr je eines Subnetzes bzw Knotenpunktes (Switch, Router) analysieren;
- entweder online mit Echtzeit- bzw Nahzeit-Analyse -oder- offline zur nachträglichen Untersuchung von Trace-Dateien, z.B. im Rahmen forensicher Analyse nach einem Security Incident.

synalyst unterstützt alle Netzwerk-Techniker und -Administratoren, die es gewohnt sind, mit Wireshark Datenverkehr aufzuzeichnen und zu sichten bzw zu analysieren.

Das MintMagic Analyse-Modul kann voll-automatisch riesige Datenmengen untersuchen, online wie offline, und umfassende Berichte erzeugen (Event Log; Tabellen und Listen; Baum-Strukturen).

Sowohl die Menge der verarbeiteten Daten wie auch Art, Umfang und Inhalt der MintMagic Berichte stellen einen massiven Mehrwert gegenüber reiner Wireshark-Nutzung dar und bringen aus unternehmerischer Sicht erhebliche Einsparung an Abreitszeit mit sich:

Die wertvolle Arbeitszeit der am besten ausgebildeten IT-Mitarbeiter (die wegen ihrer Ausbildung bei schwierigen Analysen die Arbeit übernehmen müssten) wird geschont: Statt Stunden und Tage damit zu verbingen, in Hunderten von Trace-Dateien und Millionen von LAN-Paketen nach dem Unbekannten zu suchen, reicht es mit Unterstützung von synalyst Analyse, sich mit den aussagekräftigen MintMagic Reports zu beschäftigen.

Beispiele aus der Praxis: Gefährliche Fehler, die kein SIEM je zu sehen bekam – die aber synalyst meldete

Einige Beispiele aus der synalyst Analyse-Praxis sollen verdeutlichen, worüber wir reden:

- *Beispiel aus der Praxis (1): Firewall-Problem ➧ vertrauliche Daten fließen ins Internet ab*

  Der Kunde nimmt eine neue Firewall in Betrieb. Die Analyse zeigt, dass Daten vom Intranet ins Internet weiter geleitet werden, die niemals "nach draußen" gelangen dürften. Der Firewall-Admin, darauf angesprochen, prüft die Konfiguration und bestätigt sie als "richtig": es wird "gesperrt" angezeigt. Die Analyse aber zeigt: Das Interface ist offen. Der Hersteller wird kontaktiert, und von dort wird bestätigt: Im Firewall-GUI wurden beim entsprechenen Schalter die Beschriftungen für "auf" und "zu" verwechselt: Der Admin hatte "gesperrt" konfiguriert, im Hintergrund aber war "offen", und Daten flossen ab.

- *Beispiel aus der Praxis (2): Router-Redundanz-Problem ➧ vertrauliche Daten der Geschäftsleitung auf allen Kabeln*

  Das eigentlich passive Interface eines HSRP-Doppel-Routers flutet das angeschlossene LAN-Segment mit TCP-Paketen, die eigentlich nur über das aktive HSRP-Interface weiter geleitet werden dürften, und dann auch nur in das Segment, in welchem der jeweilige Empfänger online ist; wer immer auf seinem Rechner ein Packet Capture starten kann, sieht u.a. auch vertrauliche Daten, die an die Geschäftsführung adressiert sind.

- *Beispiel aus der Praxis (3): Load-Balancer-Problem ➧ keine Ausfall-Sicherheit mehr, Betrieb im Blindflug*

  Die zwei Interfaces eines Load-Balancers ignorieren gegenseitig ihre Heartbeat-Meldungen, erkennen das aber in ihrer Management-Instanz nicht und zeigen das auch im Admin-GUI nicht an. Im Falle, dass ein Interface ausfällt, kann das andere somit nicht einspringen und nicht übernehmen, da es den Zustand des anderen nicht erkennt. Es droht unmittelbar eine schwere Betriebsstörung.

➧➧ ***Keines** der Geräte sendete eine Event-Meldung, da **keines** den eigenen Fehler-Zustand erkannte.*
***Kein Syslog**-Monitor, **kein SIEM**-System konnte daher die Fehler erkennen und seinerseits melden.*

***Fazit**: Ohne Analyse der Paket-Daten direkt am Kabel wären derlei Fehler nicht (oder nur zufällig) auffindbar.*

Weitere Ereignisse aus der Tagespraxis der **synalyst** Analyse (wahllos heraus gegriffen):

- Clients versuchen, an DMZ und Proxy vorbei direkten Kontakt zu Internet-Servern aufzubauen
- Clients versuchen, unter einander Direkt-Kontakt aufzubauen (Verdacht auf Hijacking / Malware)
- Clients senden Broadcasts auf der Suche nach irregulären Proxy-Servern (Third-Man-In-The-Middle-Attack)
- Clients annoncieren verbotene File-Sharing-Dienste im Kunden-Netzwerk
- Clients schicken ihre LDAP-Anfragen nicht etwa an den lokalen Active-Directory-Server, sondern ausgerechnet an Niederlassungen auf der anderen Seite des Planeten, über langsame Leitungen, mit langen Laufzeiten – und entsprechenden Wartezeiten und Timeout-Effekten
- Client-Identitäten ändern sich plötzlich (Verdacht auf Hijacking und/oder Malware)
- drei gegenseitig redundante DNS-Server sind falsch konfiguriert und schicken sich gegenseitig in massive Überlastung, indem sie sämtliche DNS-Anfragen von Clients in schier endlosen Forwarding-Schleifen unter einander weiter reichen
- KERBEROS-Tickets können nicht ausgestellt werden, weil Client und Server nicht Zeit-synchron sind, was wiederum auf einem Fehler in der NTP-Kette beruht, was wiederum am Funk-Empfänger hängt
- und so weiter, und so weiter

Komplexe Hintergrund-Abläufe können nicht allein aus Server-Logs, Router-Logs und Firewall-Logs erkannt werden, sondern benötigen intelligente Deep Packet Inspection – eben **synalyst** Experten-Analyse.

Datenschutz (1) – Mirror Port, VLAN, Firewall

synalyst arbeitet non-invasiv über uni-direktionale Mirror-Ports und abgetrennte VLANs.

Uni-direktional: Die Switch-Mirror-Ports geben Kopien der LAN-Pakete aus, nehmen aber nichts an.

Die am jeweiligen Mirror-Port angeschlossenen ⚙ Analyse-Agenten haben keine Möglichkeit, ihrerseits Daten ins Kunden-Netzwerk zu senden oder gar aktiv Kontakt mit Kunden-Equipment aufzunehmen.

VLANs: Die ⚙ Analyse-Agenten sowie der ⚙ Agenten-Manager und die ▼ Filter Engine arbeiten unter einander in einem abgetrennten VLAN und haben aus sich selbst heraus keinen Kontakt zum Datennetz, das sie analysieren sollen; der einzige Kontakt ins Kunden-Netzwerk ist nur möglich entweder über eine interne Firewall und/oder über die externe Firewall mit Wartungszugang auf den ⚙ Agenten-Manager.

Sicherheit: Im Gegensatz etwa zu 3rd-Party-Endpunkt-Agenten, die zur Analyse auf Clients und Servern installiert werden, und die somit direkten Zugriff auf den echten Datenverkehr und auf die Betriebssysteme haben, sind die synalyst-Komponenten abgetrennt vom Kunden-Netz und stellen folglich keine Gefahr für die Sicherheit des Kunden dar.

Das alles zusammen macht die Einrüstung völlig unkompliziert. Auch zur Vorführung oder zum Errichten eines Test-Piloten müssen keine Sicherheitsbedenken ausgeräumt werden, weil es keine Sicherheitsverletzungen geben kann (insofern nach dem oben skizzierten Muster vorgegangen wird).

Dies ist von erheblicher Bedeutung. Kaum ein anderes Analyse-Framework kann so schnell live gehen.

Datenschutz (2) – DSGVO im Analyse-Umfeld

Datenschutz-Probleme (DSGVO) bestehen in aller Regel nicht:

Die Daten verbleiben im Hause des Kunden und werden ausschließlich auf der Hardware des Kunden verarbeitet.

Der Kunde bleibt also jederzeit Herr aller Daten, nach den hauseigenen Regeln.

Die synalyst Analyse kommt allgemein erst dann in Berührung mit Datenschutzregeln, wenn z.B. Anwender private Mails im Klartext über das Unternehmensnetz senden. In solchen und ähnlichen Fällen greifen die Regeln des Kunden (etwa: Betriebsvereinbarung; Sichtung nur im Beisein des Datenschutzbeauftragten; etc).

In der Praxis hat sich bislang derlei noch niemals als Problem heraus gestellt:

- Der Fernwartungs-Zugang via Kunden-Firewall lässt keine Datei-Übertragung zu (nur Video)
- Die seitens Synapse beauftragten Mitarbeiter werden zur Verschwiegenheit verpflichtet.
- Kundenseitig haben nur ausgesuchte Mitarbeiter Zugriff auf das Analyse-VLAN bzw auf die Analyse-Rechner

Mit solchem Handlungsrahmen ist sicher gestellt, dass keine Kunden-Daten über den Analyse-Zugriff abfließen.

Datenschutz (3) – Anonymisierung & Pseudonomisierung der Berichte

Datenschutz ist auch gefordert, wenn Berichtsdaten weiter gegeben werden sollen an externe Gutachter:

Man will über den technischen Sachverhalt eine Meinung einholen, jedoch ohne leichtfertig die MAC-Adressen, IP-Adressen, DNS-Namen etc der beteiligten Rechner offen zu legen.

synalyst Analyse kennt dieses Problem und hat Antworten dazu:

- Anonymisierung:

  Während der laufenden Analyse kann Anonymisierung der MAC-Adressen und IP-Adressen automatisch vorgenommen werden; Host-Namen werden verfremdet.

- Pseudonomisierung:

  Nachträglich können alle Berichtsdaten pseudonomisiert werden (Text-Ersetzungen).
  Hierzu gibt es ein eigenes Software-Tool innerhalb der synalyst Suite.

  Ob Event Log, Listen, Tabelle, Baum-Stukturen:
  Alle Berichts-Formate können pseudonomisiert bzw anonymisiert werden.

Die technischen Elemente der Synapse-Analyse-Suite / Aufwand & Kosten

Analyse-Agenten Software: TraceCommander (Module: CaptureWizard & MintMagic)

CaptureWizard startet und steuert die Daten-Aufzeichnung

MintMagic Analyse-Experten-System und Reporting-Modul; sendet Events per Syslog entweder an den eigenen Syslog Collector und/oder an beliebige weitere Syslog-Empfänger, darunter auch SIEM-Systeme anderer Hersteller; kann sowohl stand-alone auf Laptops von Service-Technikern laufen als auch im Verbund vieler Analyse-Agenten (Distributed Network Analysis).

Agent Manager & Syslog Collector Empfängt und speichert die Ereignis-Meldungen der Analyse-Agenten. Steuert die Ereignis-Filter einzelner oder aller Analyse-Agenten. Stellt der Event-Log Filter-Engine das Material zur Verfügung (Event-Log-Dateien). Syslog Collector und Filter Engine gemeinsam arbeiten SIEM-typisch.

Event Log Filter Engine Führt die Bibliothek der Event-Log-Filter. Durchmustert die vom Syslog Collector gespeicherten Event-Logs, priorisiert, sortiert, archiviert, macht Meldung, benachrichtigt. Ist darin stark SIEM-ähnlich, verarbeitet aber nur die Meldungen der eigenen Analyse-Agenten.

Analyse-Agenten

In allen Netzwerk-Segmenten, die zu überwachen sind, zeichnen ⚙ Analyse-Agenten den Datenverkehr auf und untersuchen die Aufzeichnungen, indem die Datenpakete sowohl einzeln wie auch in ihrem Zusammenhang betrachtet werden. Ergebnis-Formate sind: Event-Log, Tabellen, Listen, Baum-Strukturen.

Die Analyse-Agenten sind (i.d.R. virtualisierte) Windows-PCs im 19-Zoll-Schrank (RZ oder Verteilerraum).

Die Agenten arbeiten mit der Synapse-Software TraceCommander, bestehend aus den folgenden Modulen:

CaptureWizard

startet und steuert die Aufzeichnung des Datenverkehrs und das Abspeichern in Trace-Dateien; im Hintergrund wird hierzu das Wireshark-Modul TShark verwendet; die Aufzeichnung erfolgt im offenen libpcap-Format innerhalb eines Ring-Buffers.

MintMagic

analysiert als Experten-System die aufgezeichneten Trace-Dateien, erzeugt und archiviert Analyse-Berichte und sendet Benachrichtigungen über bestimmte Ereignisse/Ergebnisse; dies geschieht wahlweise mit Syslog und/oder E-Mail (im RAR-verschlüsselten Anhang).

Die Analyse-Agenten kommunizieren mit dem zentralen Management-System, das zugleich seinerseits die Analyse-Agenten per Fernbefehl und je nach Anlass mit veränderlichen Ereignis-Filtern bestückt.

Die vom CaptureWizard gestartete Aufzeichnung verwendet einen sog. Ring Buffer.

Das bedeutet, dass der Trace-Aufzeichnung ein bestimmter Festplatten-Platz zugewiesen wird; innerhalb dieses Platzes werden Trace-Dateien abgelegt; ist der Platz erschöpft, werden die ältesten Trace-Dateien gelöscht zu Gunsten neu erzeugter Trace-Dateien. Dieser Ring Buffer kann je nach Platten-Kapazität und Netzwerk-Datenaufkommen als Semi-Archiv das Abbild von Tagen, Wochen, Monaten enthalten. Somit liegen im Falle von Störungen oder Security Incidents die Daten vor, die für eine forensische Analyse benötigt werden.

Hallo-Agenten

Auf den Analyse-Agenten laufen neben der Analyse-Software parallel kleine Hallo-Agenten, die alle 60 Sekunden dem zentralen Agenten-Manager per "Hallo"-Meldung anzeigen, dass der Analyse-Rechner noch lebt und erreichbar ist.

Dies ist von Belang, wenn – was unwahrscheinlich, aber nicht unmöglich ist – die Analyse-Software einmal hängen sollte und sich nicht mehr selbst beim zentralen Agenten-Manager melden kann.

Agent Manager & Syslog Collector

Der zentrale Syslog-Collector empfängt von allen Analyse-Agenten bzw deren MintMagic-Modulen die via Syslog gesendeten Ereignis-Meldungen und speichert sie in einem zentralen Event-Log ab.

Dieses zentrale Event-Log wird sodann von der Event Log Filter Engine durchmustert (s.u.).

Der Agenten-Manager zeigt den Betriebszustand der Analyse-Agenten an (Name, IP-Adresse, Software-Version, Analyse-Status, Fehler-Status, Ereignis-Filter, Uhrzeit der letzten Hallo-Meldung etc.).

Der Agenten-Manager kann an einzelne oder alle Analyse-Agenten neue Ereignis-Filter senden bzw verteilen, wodurch per Mausklick an allen MessPunkten tagesaktuelle bzw bedarfsaktuelle Filter gesetzt werden können. Diese Filter sind – technisch gesehen – Text-Filter auf das jeweilge MintMagic Event Log.

Weiterhin kann vom Agenten-Manager aus per Mausklick via RDP oder SMB auf die Agenten und ihre Daten zugegriffen werden. Außerdem können E-Mail-Tagesberichte (RAR-verschlüsselt) versendet werden.

Filter Engine (Library & Archive)

Das vom zentralen Syslog-Collector aufgezeichnete Event Log ist zu umfangreich, um von Anwendern in Handarbeit gesichtet zu werden. Sichtung, Priorisierung, Filterung erfolgen daher maschinell.

Dies erledigt die Filter Engine.

Sie durchmustert die Event-Log-Dateien des jeweiligen Vortags.

Hierzu wird eine Filter-Bibliothek geführt. Sie ist bei Auslieferung bzw Erst-Installation mit Standard-Filtern vorgefüllt; im Laufe der Arbeiten kommen neue Filter hinzu, welche die Besonderheiten des Kunden-Umfelds abbilden bzw nach genau den Fehlern und Ereignissen suchen, die für das LAN/WAN des Kunden typisch sind. Es können mehrere Hundert Filter-Definitionen verwaltet werden.

Die Einträge der Filter-Bibliothek können mit verschiedenen Prioritätswerten versehen sein, um wichtige von unwichtigen zu unterscheiden.

Der tageweise arbeitende Filter-Lauf kann sich auf alle verfügbaren Filter-Definitionen erstrecken -oder- nur auf die aktiven Filter (unter Auslassung der inaktiven Filter) -oder- nur auf eine bestimmte Teil-Menge (etwa: nur DNS; oder: alle Filter, die eine bestimmte IP-Adresse betreffen; etc).

In einer Ergebnis-Liste wird festgehalten, welche Filter wie viele Treffer ergaben, und wann genau das letzte Treffer-Ereignis stattfand. So könnte z.B. aus der Treffer-Liste schnell heraus gelesen werden, wann das letzte Ereignis mit KERBEROS-Ablehnung auf Grund falscher TimeStamp-Übergabe (Fehler in der Zeit-Synchronisation des Clients) an welchem Tag zu welcher Uhrzeit stattfand bzw nachweisbar war.

Jeder Filter kann seine Ergebnisse an hinterlegte Empfänger versenden (E-Mail, RAR-verschlüsselt).
Am Ende eines jeden Filter-Laufs kann die Gesamt-Treffer-Liste ebenso versendet werden.

Aufwand, Kosten, Einstieg: maximal niederschwellig, maximal ergiebig

Der Aufwand zum Einrüsten ist sehr begrenzt; in wenigen Stunden kann das System aufgesetzt werden.

Analyse-Agenten	bestehen aus Windows-Rechnern, die der Kunde zur Verfügung stellt. Da vielerorts bereits in den 19-Zoll-Schränken PC-Hardware mit Virtualisierungs-Plattform arbeitet (z.B. VMware), ist ggf der Aufwand zur Bereitstellung eines Analyse-PCs sehr gering, sowohl finanziell wie auch personell und zeitlich. Sobald der Zugriff frei geschaltet ist, installiert Synapse die Software, schaltet sie frei, konfiguriert sie – und die Analyse läuft.
Agenten-Manager	Der zentrale Agenten-Manager / Syslog-Collector ist schnell installiert.
Syslog-Collector	Er lernt automatisch aus den eingehenden Syslog-Meldungen die Namen und IP-Adressen der Analyse Agenten.
Filter Engine	Die Event-Log Filter-Engine mit ihren mitgelieferten Standard-Filtern ist ebenfalls schnell betriebsfähig. - Die Pflege dieser Filter ist später Kern des Services.

Da die Analyse an uni-direktionalen Mirror-Ports stattfindet (stattfinden sollte), haben die Analyse-Agenten keinen aktiven Zugriff aufs Netzwerk des Unternehmens; gleiches gilt für den Agenten-Manager und die Filter Engine.

synalyst arbeitet folglich non-invasiv.

Daher kann auch eine Vorführung oder ein Test-Pilot sofort und aus dem Stand aufgebaut werden, ohne dass die Kunden-Sicherheitsprotokolle zur Einbettung aktiver Systeme zu greifen hätten.

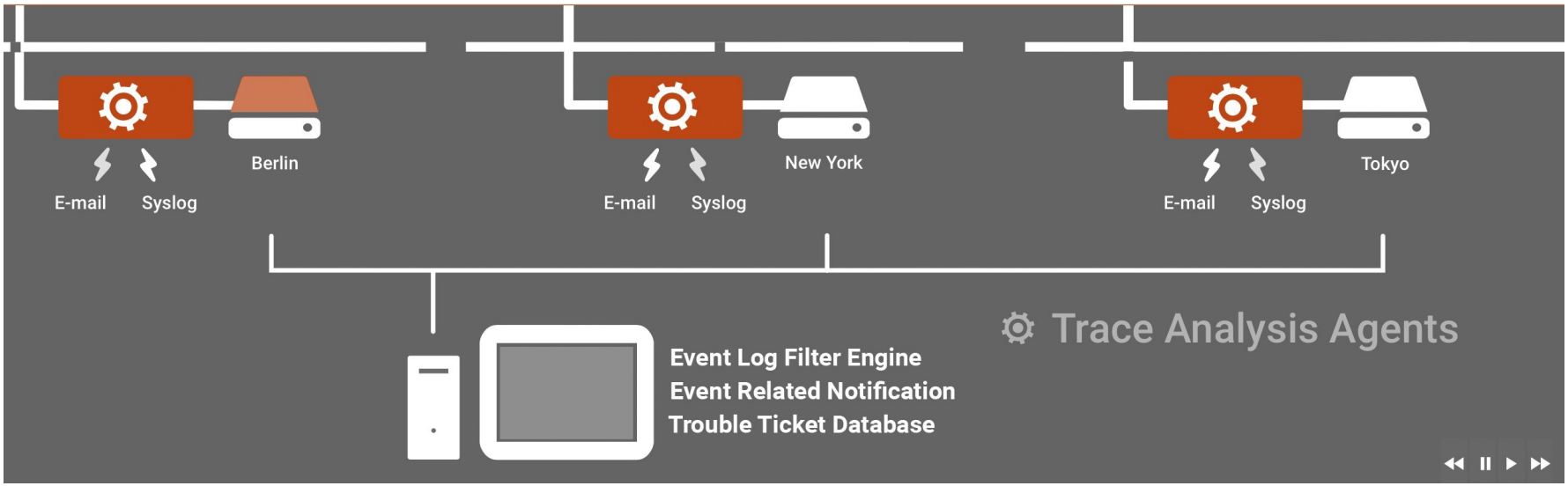
Impressum

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