synalyst

smart network analysis

Skizze einer Zusammenarbeit zwischen

Synapse Networks GmbH

und

IT-Kunden mit LAN-WAN-Netzwerken

smart network analysis

Inhaltsverzeichnis

IT-Kunden und der Schutz ihrer LAN-WAN Netzwerke

Ausgangslage: Verbesserung von Verfügbarkeit und IT-Sicherheit durch Analyse

Jedes **Unternehmen mit IT** verarbeitet schutzwürdige Daten und ist daher angewiesen auf IT-Security.

Der Einsatz üblicher Mittel wie Firewall, Intruder Detection System (IDS), Privileged Session Management (PSM), Security Information and Event Management (SIEM) etc ist notwendig und hilft, reicht aber nicht aus. Meldungen aus solchen Instanzen sind, mathematisch gesprochen, oft nur zweite oder dritte Ableitung des Original-Ereignisses, und sie sagen oft zu wenig über Ursache und Hergang verdächtiger Vorfälle.

In das Standard-Portfolio der IT-Sicherheit passt daher ein zusätzlicher Dienst: LAN-Analyse in Form von Deep Packet Inspection: Datenpakete/Datenflüsse werden durch ein Experten-Sytem darauf hin untersucht, ob technische Fehler, Konfigurationsprobleme oder Gefahren für Sicherheit und Integrität vorhanden sind.

Viele der üblichen Methoden sind vorwiegend oder gänzlich reaktiv, da sie (in gewisser Weise: lediglich) bereits aufgetretene Ereignisse erfassen – wenn es also ggf bereits zu spät ist.

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; oder indem Fehler erkannt werden, die von anderen Schutz-Komponenten gar nicht erkannt werden (können) (*s.u.: Praxis-Beispiele*).

Mit der **synalyst** Software-Suite können **IT-Kunden** Verfügbarkeit und Sicherheit erhöhen.

Vorführung und Leistungsnachweis: schnell und wirkungsvoll

Jeder **IT-Kunde** will seine Mittel möglichst wirkungsvoll einsetzen – daher ist der Nachweis, dass **synalyst** Analyse leistungsfähig ist und bedarfsgerecht arbeitet, mit sehr geringem Einsatz an Personal, Zeit und Mitteln möglich. Es werden nur wenige Betriebsmittel für Pilot-Projekte gebunden.

Eine Vorführung hat nicht nur den Wert für die IT-Sicherheit, sondern hat auch die Effizienz zu zeigen.

Die **synalyst** Analyse benötigt für einen ersten Einsatz vor Ort:

1 Switch-Admin zum Setzen des Mirror-Ports
1 Switch-Mirror-Port *-oder-* Trace-Daten aus vorigen Aufzeichnungen
1 PC/Laptop mit der **synalyst** Analyse-Software
1 Beamer im Besprechungsraum (oder Video-Session bei Fernzugriff)
1 Vormittag/Nachmittag Zeit für die Live-Analyse und/oder für die Sichtung der Analyse-Ergebnisse

Ob die Trace-Daten live vom Mirror-Port kommen oder zuvor aufgezeichnet werden, kann wahlweise entschieden werden. Wichtig ist, dass die Aufzeichnungen "frisch" sind (also tagesaktuell).

Unser Anspruch ist: Im Rahmen eines Vormittags oder Nachmittags nachzuweisen,

- dass **synalyst** Analyse Dinge aufdeckt, die bis dahin nicht bekannt waren und abgestellt gehören;
- dass **synalyst** Analyse leistet, was gefordert ist:
  schnell, umfassend und verständlich Erkenntnisse zu vermitteln und Handlungsfähigkeit herzustellen.

Mit geringstmöglichem Aufwand und in kurzer Zeit vor Ort und live den Nachweis zu erbringen, dass Bedarf besteht, und dass der Bedarf mit **synalyst** Analyse gedeckt werden kann: das ist unser Anspruch.

Nutzen im späteren Tages-Betrieb

Der **IT-Kunde** bekommt von Synapse das Angebot eines Managed Services zur Dauer-Analyse.

Über alle Schichten der Kommunikation (OSI-Modell) erfolgt mit **synalyst** dauerhafte automatische Analyse und Berichts-Erzeugung samt Meldung an hinterlegte E-Mail-Adressen.

Synapse betreibt per Fernzugriff die Analyse-Agenten, die zentrale Sammlung und Speicherung der Ereignis-Meldungen sowie die Filterung dieser Meldungen nach mehreren Hundert Kriterien.

Die Analyse läuft ausschließlich im Hause des Kunden und ausschließlich auf Hardware des Kunden.

Die Ergebnisse der **synalyst** Analyse ...

- helfen, Fehler zu erkennen, bevor sie zu Störfällen ("incidents") werden;
- 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 sichert ab und ist pro-aktiv. Gleichzeitig ermöglichst sie forensische Analyse.

Dieser Ansatz macht für **IT-Kunden** die Zusammenarbeit mit **Synapse** interessant.

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.

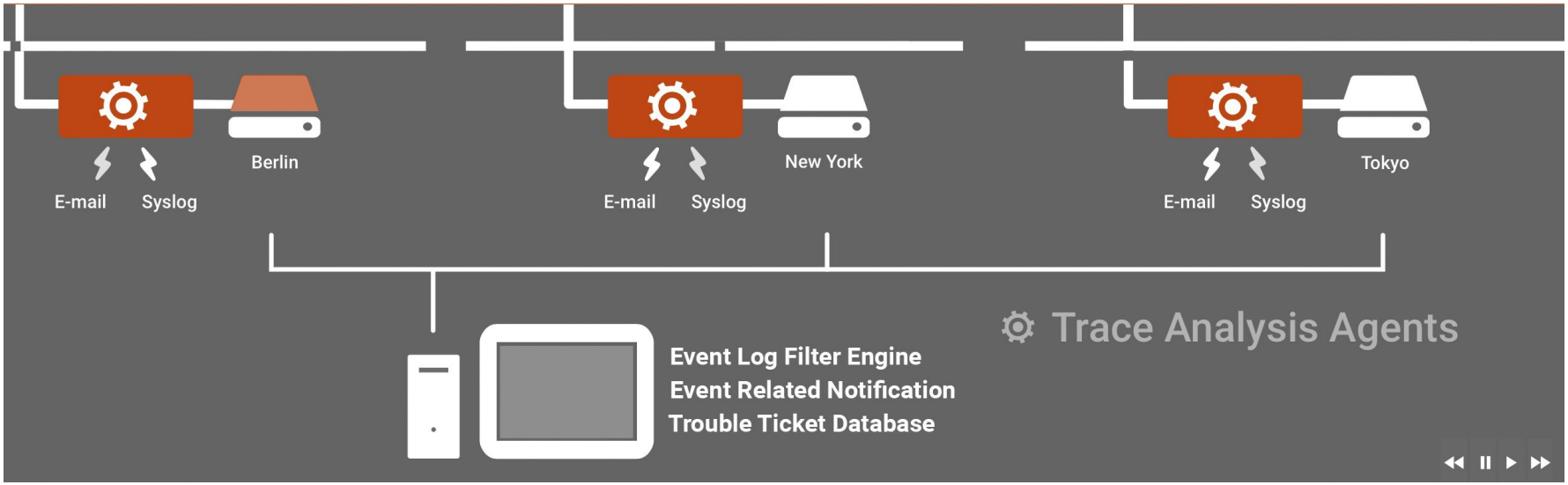
Firewall, Intruder Detection System, Server Log etc sowie die mit Meldungen aus dieser Quelle gefüllten SIEM-Systeme zeigen nur das, was anderswo erkannt und wie-auch-immer gedeutet und gewichtet wurde.

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.

Weltweite Analyse mit synalyst: ca 30 Agenten, ca 20 Mio Events, ca 400 Fehler-Filter



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;
auf diese Art werden die gemeldeten Ereignisse sortiert, priorisiert, ablegt und in Berichten zugänglich macht.

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 einerseits innerhalb der eigenen Software-Suite ähnlich und zunächst einmal stand-alone; 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. Vorhandene SIEM-Systeme werden stark "gefüttert" 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).

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

Agent Manager & Syslog Collector

Empfängt und speichert die Ereignis-Meldungen der Analyse-Agenten. Steuert die Ereignis-Filter einzelner oder aller Analyse-Agenten.

Event Log Filter Engine

Führt die Bibliothek der Event-Log-Filter. Durchmustert die vom Syslog Collector gespeicherten Event-Logs, priorisiert, sortiert, macht Meldung, benachrichtigt.

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 Event-Log-Filter können von der Zentral-Konsole per Mausklick an alle Analyse-Agenten automatisch verteilt werden, was wiederum den Syslog-Rückfluss zur Zentral-Konsole steuert.

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.

Ist die Datenrate auf der Leitung sehr hoch, kommen also über den Mirror-Port mehr Packets zum Analyse-Agenten, als dieser in Echtzeit/Nahzeit verarbeiten kann, werden einzelne Trace-Files übersprungen. Das führt kurzfristig zu Verlusten, die aber durch die langfristige 24/7/365-Analyse ausgeglichen 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 / Data Aggregator

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

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

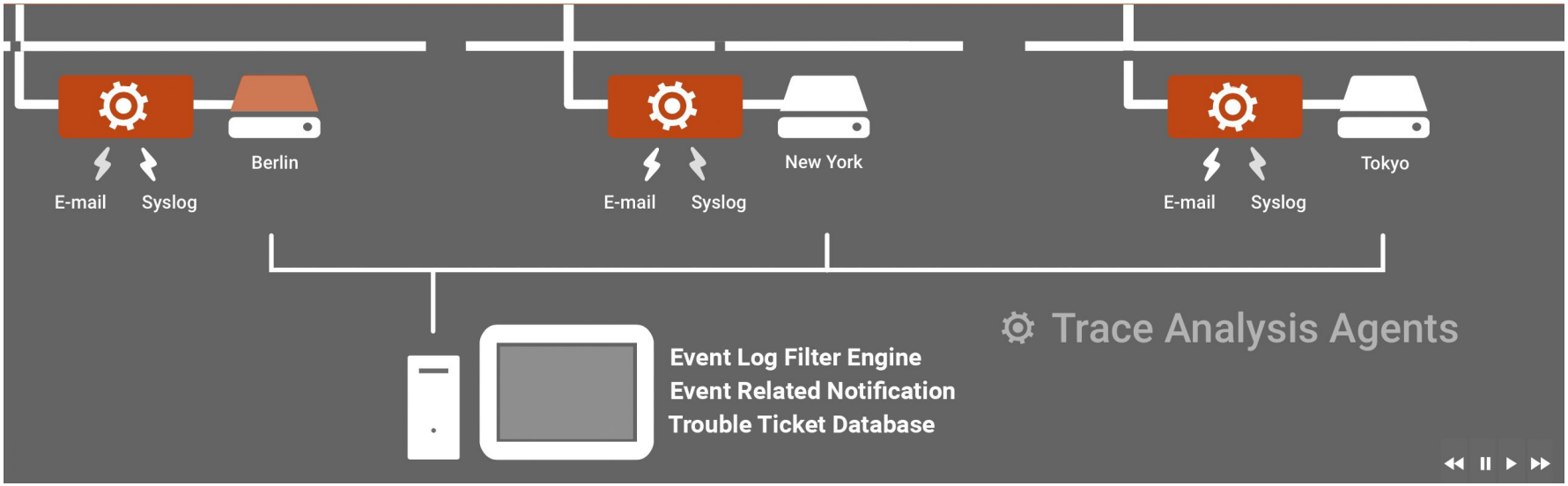
Synapse Networks GmbH
Peter-Bischof-Str. 2A
55435 Gau-Algesheim

fon: 06725-9990710

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

Kunden-Kontakt:

office-contact@synalyst.net



www.synalyst.net

ANHANG: Leistungen + Merkmale

Überblick: Darstellung von Analyse-Fähigkeiten und -Ergebnissen (nicht vollständig, beschränkt auf die gängigsten).

Host-ID-Datenbank / MAC-IP-Adresse(n), ComputerName, FQDN, Identitäten

In der zentralen Host-ID-Datenbank werden MAC-Adressen, IPv4/IPv6-Adressen, ComputerNamen, DNS-Namen, WINS-Namen, NetBIOS-Namen, DHCP-Client-Namen, DHCP-Hersteller-Kennung, Windows-Benutzernamen, SNMP-Gerätenamen (u.v.m.) erfasst, dies sowohl auf jedem Analyse-Agenten wie auch auf der zentralen Sammel-Konsole.

Die Datenbank ist abfragbar, die Ergebnisse können über Include/Exclude-Filter eingegrenzt werden. Jedem Host-Datensatz sind die Namen und IP-Adressen derjenigen Analyse-Agenten zugeordnet, von denen die jeweilige Information stammt, wodurch der Standort eines jeden Hosts sichtbar wird bzw ermittelt werden kann, welcher Analyse-Agent einem gesuchten Host/Device am nächsten ist. In der Datenbank ist mit Datum vermerkt, wann welches Identifikationsmerkmal eines Geräts durch welches Protokoll zuletzt in der Analyse erkannt und an die Datenbank gemeldet wurde. Sollten Identitäten nicht eindeutig sein, mehrfach verwendet sein bzw wechseln, so wird ist dies in den Datensätzen sichtbar und wird seitens der Analyse-Agenten im jeweiligen Event-Log ausgegeben.

Das Filtern erlaubt die gezielte Suche z.B. nach Mobile Devices, SNMP-Komponenten oder allen Servern, die über einen bestimmten UDP/TCP-Port arbeiten, oder nach allen Geräten, die zu einer bestimmten DNS-Domain gehören oder die in einem bestimmten IP-Subnetz siedeln.

Dadurch, dass in jedem Host-Datensatz vermerkt ist, welcher Analyse-Agent die Daten geliefert hat, und mit welchem IP-TTL-Wert die IP-Pakete des Hosts am MessPunkt vorbei gekommen sind, lässt sich leicht erkennen, welcher Analyse-Agent dem Host am nächsten ist bzw welcher Analyse-Agent im Idealfall direkt im selben IP-

Subnetz bzw LAN-Segment siedelt wie der gesuchte Host. Auf diese Weise lässt sich schnell erkennen, welcher Analyse-Agent bei Bedarf das lokale Verhalten des Hosts mittels Capture-Traces belegen kann.

Diese Fähigkeit, die geeigneten MessPunkte bzw Analyse-Agenten zu ermitteln, ist von großer Bedeutung:

> Falls der Verdacht besteht, dass ein Rechner infiziert ist und versucht, die Nachbarn im selben LAN-Segment bzw IP-Subnetz zu infizieren (ohne einen Router oder eine Firewall überqueren zu müssen, was dort auffallen könnte), ist es unbedingt wichtig, das lokale Verhalten nachweisen zu können, heißt: 100% aller Pakete zu sehen, die dieser Rechner sendet und empfängt (und nicht nur solche Pakete, die über einen Router in andere Segmente gesendet werden).
>
> Falls der Verdacht besteht, dass die Verbindung zwischen zwei Rechnern gestört ist, und wenn diese Verbindung über eine Vielzahl von Switches, Routern und Firewalls läuft, so ist zur zweifelsfreien Analyse wichtig, exakt zu erkennen, an welchen MessPunkten bzw Analyse-Agenten die IP-Pakete dieser Verbindung vorbei kommen. Diese Frage lässt sich durch gezielte Suche in der Host-ID-Datenbank beantworten. Hintergrund ist u.a., dass nicht in jedem Falle gesichert ist, dass die IP-Route durchs Netzwerk so verläuft, wie sie der Plan des Betreibers vorsieht. Es besteht im Einzelfall die Möglichkeit, dass die IP-Route über Knoten verläuft, die dafür nicht vorgesehen waren/sind. Um derlei abzuklären, sind Abfragen der Host-ID-Datenbank hilfreich und erforderlich.

Die Host-ID-Datenbank kann bis zu 65.545 Datensätze aufnehmen und kann auf lokale Adressen beschränkt werden; die Datenbank kann also betrieben werden wahlweise mit oder ohne Fremd-IP-Adressen etwa aus dem Internet oder aus verbundenen Partner-Netzwerken.

Benutzer-Namen / Logon-Namen

Eine Vielzahl von Protokollen wird analysiert, um Benutzer-Namen und Logon-Namen zu ermitteln, die im Netzwerk zum Zwecke von Authorization/Authentication verwendet werden. Dazu zählen u.a.:

- LDAP / Active Directory
- KERBEROS
- SMTP / E-Mail
- SMB / Windows Logon
- HTTP / Proxy Authentication
- RADIUS / Remote Logon
- VoIP / SIP
- SQL / Oracle MySQL

Zu jeder Identität werden der ermittelnde Analyse-Agent sowie die Uhrzeit des Vorkommnisses vermerkt.
Dies erlaubt in starkem Maße Kontrolle darüber, welche Anwender-Kennungen wann wo verwendet wurden.

White List / Black List

MAC Adressen können in einer White List erfasst werden.
MAC-Adressen, die im LAN auftreten und nicht in der White List hinterlegt sind, werden als Intruder gemeldet.
IP-Adressen können zusätzlich mit UDP/TCP-Ports in White List / Black List abgelegt werden.
Server können separat in White List und Black List abgelegt werden.
Die MAC/IP-Adressen können anfänglich automatisch mit allen erkannten Adressen gefüllt werden.
Im Ergebnis unterstützen *White List / Black List* die Erkennung von *IP Intruder / IP Jailbreak* (s.u.).

MAC Adressen

Alle MAC-Adressen werden erfasst und in Tabellen ausgegeben mit Rx/Tx-Statistiken.

MAC-Adressen, die zu Routern oder Firewalls gehören, werden gesondert ausgewiesen.

MAC-Adressen von Absendern, deren Pakete durch Flutung ins LAN kommen, werden erkannt und gemeldet. Grund ist, dass Switch-Fehler (table overflow) zu massiven Flutungen von LAN-Segmenten führen können.

MAC-Adressen, die als Absender auffällige bzw verdächtige Multicast/Broadcast-Rundrufe verschicken, werden gesondert erfasst.

WLAN Adressen

WLAN-Controller tauschen unter einander Tabellen aus mit MAC-Adressen und Namen von WLAN-Teilnehmern. Im Falle von Cisco-WLCCP werden diese Daten erfasst und in Tabellen ausgegeben.

ARP Adressen

Alle ARP-Adressen werden erfasst und in Tabellen ausgegeben (aktuell nur IPv4).
Ist die Zuordnung von MAC/IP-Adresse(n) nicht eindeutig und/oder wechselnd, wird dies erkannt/gemeldet.

IP Adressen

Alle IPv4/IPv6-Adressen werden erfasst und in Tabellen ausgegeben samt (im Falle von IPv4) Rx/Tx-Statistiken.
Ist die Zuordnung von MAC/IP-Adresse(n) nicht eindeutig und/oder wechselnd, wird dies erkannt/gemeldet.
Ebenso richtet sich die Analyse auf:

- IP Address Scan (ggf Vorbereitung eines Angriffs durch interne oder externe Maschinen)

IP Matrix

Alle IPv4-Dialog-Paare werden in einer Tabellen-Matrix erfasst: wer hat mit wem wie viele Packete ausgetauscht und mit welchen Protokollen (UDP, TCP, ICMP, etc) und mit welchen TCP-Sitzungs-Besonderheiten (Abbruch etc).

IP Idle Time

IP-Adressen, die als Absender längere Zeit inaktiv waren, werden erkannt und gemeldet (Schwellenwert).

IP Routing

Wenn sich IP-Routen zwischen Tx-Host und Rx-Host ändern (auf der Teilstrecke vom Tx-Host bis zum Analyse-Agenten), so wird dies erkannt und gemeldet.

Für jede IPv4-Adresse wird in einer Tabelle nachgewiesen, über wie viele Router die IP-Pakete eines jeden Absenders bis zum Standort des Analyse-Agenten gelaufen sind, wodurch auch wechselnde Zahlen der Router-Hops sichtbar werden. Wechselnde Router-Hop-Counts können ggf Hinweise auf Fehler oder ungünstige Load-Balancing-Konfiguration sein.

Routing-Loops zwischen Routern werden erkannt und gemeldet.

Alle Router, sofern sie sich am jeweiligen Analyse-Agenten sichtbar machen, werden erfasst und gelistet.

Router, die mit i.d.R. veralteten IP-Helper-Einträgen arbeiten, werden erkannt und gemeldet. Grund hierfür ist, dass durch IP-Helper ggf Broadcasts/Multicasts von einem Subnetz ins nächste weiter gegeben werden, was im schlechtesten Falle zu Flutungen und Loops führen kann.

Bei Routing-Redundanzen (Beispiel: Cisco HSRP) wird in der Analyse überwacht, ob als passiv konfigurierte Router-Interfaces wirklich passiv sind/bleiben oder trotz der Passiv-Einstellung IP-Pakete übermitteln bzw fluten. Dies darf theoretisch nicht vorkommen, wurde aber bereits in der Praxis beobachtet.

IP Router & Protocols

Die in der Analyse verarbeiteten Router-Exchange-Protocols sind IP-RIP, IPX, VRRP, OSPF, HSRP.

Auf Grund der Dominanz bzw der überwiegenden Verbreitung wird hauptsächlich HSRP analysiert.

Die seltenen und/oder veralteten Protokolle werden nicht in der selben Tiefe wie HSRP verarbeitet.

IP NAT Network Address Translation (trusted/untrusted)

Interne IP-Adressen werden nur intern verwendet; zum Internet hin werden öffentliche IP-Adressen verwendet; die Umsetzung bzw der Wechsel der IP-Adressen durch Router bzw Proxy-Server gehört zu den Basis-Techniken des Internets.

Bestimmte Protokolle erlauben unter bestimmten Umständen, die hinter einer NAT-Instanz verwendete, interne IP-Adresse eines Teilnehmers zu erkennen, wenn/obwohl der MessPunkt der Analyse außerhalb der NAT-Instanz liegt.

Die Analyse kann in bestimmten Fällen dennoch die interne Adresse sichtbar machen.

IP Tunneling (VoIP/SIP)

Insbesondere Voice-over-IP (VoIP) bzw SIP benötigen spezielle Signalisierungen, um zwischen Endgeräten Verbindung herzustellen, die in den verschiedensten IP-Teilnehmernetzen siedeln - Netze, die normalerweise mit Firewalls wie Fort Knox gesichert sind. Um Internet-Telefonie zwischen zwei Tischgeräten zweier verschiedener Unternehmen zu ermöglichen, bedarf es eines gesonderten "Freie-Fahrt"-Schaltung, in diesem Zusammenhang "Tunnel" genannt. Das hierzu verwendete STUN-Protokoll wird voll analysiert.

Fehler, ihre Gründe und die beteiligten Systeme (Router, Firewalls) werden detailliert protokolliert.

IP Tunneling (PPPoE,GRE, EtherIP, etc)

Echtes IP-Tunnelling verschiedenster Art wie PPPoE, GRE, EtherIP, WLAN/CAPWAP/IEEE-802.11, etc wird in der Analyse ebenfalls erkannt und entsprechend verarbeitet.

Verschlüsselte Tunnel sollen und können **nicht** in der Analyse entschlüsselt werden.

IP Trusted Networks

Die Analyse erkennt anhand verschiedenster Konfigurations-Meldungen in BOOTP, DHCP, DNS, KERBEROS, LDAP etc, welche IP-Netze bzw IP-Subnetze als vertrauenswürdig gelten bzw Teil der Betreiberlandschaft sind.

Sollten IP-Teilnehmer aktiv werden, die nicht diesen vertrauenswürdigen Subnetzen angehören, kann dies ein unerwünschtes Ereignis sein; es wird erkannt und gemeldet. Siehe -> Intruder / Jailbreak.

IP Same Subnet Session (TCP/UDP)

Typischerweise siedeln Clients und Server in unterschiedlichen IP-Subnetzen, getrennt/verbunden über Router und Firewalls. In Client-Subnetzen ist daher davon auszugehen, dass es **nicht** zu Verbindungsversuchen kommt zwischen zwei IP-Teilnehmern, die im selben IP-Subnetz siedeln.

Die Analyse erkennt sucht gezielt nach solchen Quer-Verbindungen zwischen Client-Subnetz-Nachbarn.

In Client-Subnetzen wird jegliche Aktion dieser Art via TCP/UDP als Verdachtsfall angesehen auf Weitergabe einer Virus-Infektion und/oder einer Ausforschung von Sicherheitslücken und Daten.

In Server-Subnetzen können Same-Subnet-Sessions verdächtig sein, müssen es aber nicht, da typischweise Server untereinander Daten austauschen bzw abgleichen, so etwa für Redundandy-Sync.

IP Intruder / IP Jailbreak

Verdachtsfälle werden protokolliert, bei denen ggf vertrauens**un**würdige IP-Adressen von außen ins lokale Netzwerk einwirken, oder bei denen interne IP-Teilnehmer versuchen, ggf vertrauens**un**würdige IP-Adressen extern anzusprechen.

Zur entsprechenden Bewertung tragen u.a. die oben genannten *IP trusted networks* bei sowie die ggf aktivierten *White Lists / Black Lists* (s.o.).

Im Event Log werden auch Vorbereitungs-Handlungen für den Ausbruch vermerkt, und in Report-Listen werden die beteiligten Rechner samt Vorgehensweise erfasst; siehe unten -> *IP Backdoor (LAN, WLAN, Mobile Device, Internet).*

Beispiele von IP Jailbreak (Ausbruchsversuche):

-1-
Eine Überwachungskamera im Server-Raum versucht, eine IP-Adresse in Asien anzusprechen; diese Server-IP-Adresse gehört nicht in die Gruppe der o.g. IP Trusted Networks. So gesehen im Jahr 2023.

-2-
Mehrere Überwachungskameras in verschiedenen Server-Räumen versuchen, sich mit einem WLAN zu verbinden bzw bieten WLAN-Verbindungen an, obwohl der Betreiber dergleichen nicht konfiguriert / nicht zugelassen hat. So gesehen im Jahr 2023.

-3-
Eine Video-Konferenz-Anlag versucht, an der bestehenden Struktur mit Firewalls und Proxy-Servern vorbei Verbindung aufzubauen zu Servern im Internet. Es stellt sich heraus, dass sich dieses Verhalten nicht unterdrücken lässt. In der Folge werden diese Anlagen ersetzt durch neue, die das Verhalten entweder zuverlässig nicht zeigen, oder bei denen es sich zuverlässig abschalten lässt. Der Betreiber steht vor der schwierigen Wahl, ob er die wirtschaftlich vorberechnete Betriebsdauer abwartet, bis die Ersatz-Beschaffung einsetzt, oder den

wirtschaftlichen Verlust in Kauf nimmt und sofort in die Ersatz-Beschaffung eintritt (Sicherheit vs Kosten). So ereignet im Jahr 2020 in einer Außenstelle in Asien.

-4-
Eine Video-Konferenz-Anlage ist nicht, wie vorgesehen, nur via WLAN ans Kommunikationsnetz angeschlossen (und dort insbesondere auch für Gast-Benutzer erreichbar), sondern versehentlich auch mit einem LAN-Kabel mit dem Campus-Netz verbunden. Dadurch besteht die Möglichkeit (je nach Konstruktion bzw etwaiger Kompromittierung des Devices), dass eben diese Gast-Benutzer ins Campus-Netz gelangen könnten bzw Daten aus dem Campus-Netz via WLAN nach außen abfließen könnten (Internet Backdoor). Die Analyse liefert den Hinweis. Das LAN-Kabel wird sofort gezogen. So gesehen in 2022.

-5-
Ein IP-Internet-Radio, das sich ein Anwender ohne Genehmigung privat auf seinen Dienst-Schreibtisch gestellt hat, ist nicht nur mit dem ungeschützten Gast-WLAN verbunden (was ohne Genehmigung zugelassen ist), sondern auch via LAN-Kabel mit dem Campus-LAN. Das Internet-Radio könnte dadurch eine Internet-Backdoor öffnen, interne Daten könnten nach außen abfließen. Die Analyse liefert den Hinweis. Das LAN-Kabel wird sofort gezogen. So gesehen 2021.

-6-
Clients versuchen, Zugriffe auf Internet-Server einzuleiten nicht über den vorgesehenen Weg via Proxy-Server, sondern direkt; hierzu werden DNS-Anfragen gesendet, um die IP-Adressen der Internet-Server zu ermitteln; danach folgen ggf TCP/UDP-Sendungen zwecks Aufbau einer Verbindung. Dieses Verhalten ist ständig zu beobachten, da es beispielsweise von Microsoft verwendet wird, um für das Windows-Betriebssystem zu ermitteln, ob eine direkte Internet-Verbindung besteht (oder nicht), wesentlich zwecks Steuerung des Update-Verhaltens. In diesem Grundrauschen können sich andere Versuche verstecken, die nicht so freundlich gemeint sind. Um hier Gut+Böse scheiden zu können, werden die Verbindungsversuche - sofern möglich - gekennzeichnet mit den DNS-Namen der beteiligten Rechner. Da der Ansprache eines Internet-Servers i.d.R. eine DNS-Auflösung voraus geht, sind IP-Adresse und DNS-Name in der o.g. Host-ID-Datenbank enthalten, werden abgefragt und

dem Event-Log zugefügt. Hat es keine DNS-Abfrage gegeben, könnte es sein, dass die IP-Adresse des Internet-Servers im Application Code direkt hinterlegt ist, was teils von Microsoft getan wird, um DNS-Spoofing auszuschließen, teils aber auch von Angreifern getan wird, um nicht durch DNS-Anfragen aufzufallen, die sich auf "Piraten-Mutterschiffe" beziehen, die ggf in öffentlichen DNS-Blacklists hinterlegt und folglich bekannt sind. Die Analyse liefert über die Kombination von Event-Log, DNS-Tabellen, Host-ID-Datenbank und Filterungen die Verdachtsfälle sowie das Werkzeug für Sichtung und Bewertung.

IP Backdoor (LAN, WLAN, Mobile Device, Internet)

Angreifer können versuchen, eine IP-Routing-Backdoor ins Internet zu öffnen. Dies kann u.a. dadurch geschehen, dass ein Mobile Device mit dem Netzwerk verbunden wird und dieses Mobile Device dann als Router dient, das Verbindungen zwischen "außen" und "innen" herstellt, ohne dass dies die Mitarbeiter eines Unternehmens bemerken.

Auf den ersten Blick harmlose Protokolle wie ICMP, DHCP, WINS, DNS u.a.m. können dazu verwendet werden, IP Backdoors zu suchen, zu finden, zu öffnen.

Derlei Aktivitäten werden von der Analyse erfasst und gesondert protokolliert.

Und mehr noch: schon die schiere Möglichkeit, dass eine solche Aktivität einmal stattfinden könnte, insofern die Voraussetzungen dafür als gegeben erkannt werden, wird in der Analyse gesucht und, sofern vorhanden, protokolliert.

Die entsprechende Liste gehört allgemein zu den Top-10-Prioritäten der Gefahrenabwehr.
Bei Erst-Analysen bzw Test-Analysen zeigt sich immer wieder, dass hier nahezu immer die größten Lücken sind.

TCP Analyse

Es werden Rx/Tx-Statistiken für alle TCP-Ports geführt.

Es werden u.a. folgende Ereignisse bzw Zustände erkannt:

- TCP Paket-Verluste
- TCP Paket-Wiederholungen / Retransmissions (ReTx, i.d.R. Folge voran gegangener Paket-Verluste)
- TCP Pakete in verdrehter Reihenfolge (ggf als Folge wechselnder IP-Routen, s.o.)
- TCP Dialoge mit auffallenden Wartezeiten/Verzögerungen bzw Latenz-Zeiten (siehe unten)
- TCP locally routed - Datenpaket ist doppelt im Trace, erst vor, dann nach dem Router-Hop
- TCP One Way Traffic - Pakete zwischen zwei TCP-Partnern sind nur in einer Richtung zu sehen (ggf. Flooding)
- TCP Sitzungs-Versuche, die scheitern, sei es durch fehlende Server-Antwort, sei es durch Blocken/Verweigern
- TCP Sitzungs-Versuche zwischen IP-Nachbarn im selben IP-Subnetz (ggf Versuch einer Infektions-Weitergabe)
- TCP Sitzungs-Abbrüche, sei es durch den TCP-Partner, sei es durch Fehler/Ereignisse im Netzwerk selbst
- TCP Datendurchsatz pro Zeit-Einheit, Schwankungen, Maximum, Minimum, Durchschnitt, Bewertung.
- TCP Window Size bzw Steuerung des Empfangs-Puffers eines jeden TCP-Partners: Erfassung und Bewertung.
- TCP Sessions, die zwar mit Handshake zu Stande kommen, bis zu ihrem Ende aber keine Daten bewegen
- TCP Session Report nach Ende/Abbruch jeder Sitzung, sowohl im Event-Log wie auch im CSV-Format (Excel).
- TCP Port Scan (ggf Vorbereitung eines Angriffs durch interne oder externe Maschinen)
- TCP Ports je Server: Liste aller TCP/UDP-Server und aller Ports, auf denen sie aktiv antworten - oder eben nicht
- TCP Ports je Clients: Liste aller TCP/UDP-Ports, auf denen Clients Server ansprechen (bzw dies versuchen)

UDP Analyse

- UDP Sitzungs-Versuche, die scheitern, sei es durch fehlende Server-Antwort, sei es durch Blocken/Verweigern
- UDP Sitzungs-Versuche zwischen IP-Nachbarn im selben IP-Subnetz (ggf Versuch einer Infektions-Weitergabe)
- UDP Port Scan (ggf Vorbereitung eines Angriffs durch interne oder externe Maschinen)
- UDP Ports je Server: Liste aller TCP/UDP-Server und aller Ports, auf denen sie aktiv antworten - oder eben nicht
- UDP Ports je Clients: Liste aller TCP/UDP-Ports, auf denen Clients Server ansprechen (bzw dies versuchen)

TCP/IP Congestion Control

Sowohl das IP-Protokoll wie auch das TCP-Protokoll enthalten Mechanismen, die es den Teilnehmern erlauben, Signale auszutauschen, die gegenseitig Auskunft geben über etwaige Stauungen/Latenzen im Peer-to-Peer-Datenfluss. Diese sog. Congestion Control wird nicht nur von den Endsystemen (Client, Server) unterstützt, sondern auch von Routern, die ihrerseits den beteiligten Endsystemen Mitteilung geben können über Stauungen, was dann dazu führen kann/soll, dass die Endsysteme die Datenrate senken oder andere Übertragungswege suchen.

Diese Congestion Control wird durch die TCP/IP-Analyse erfasst, und etwaige Ereignisse werden im Event Log sichtbar gemacht.

Dies unterstützt die Bewertung von Anwender-Aussagen "das Netzwerk ist langsam".

TCP Latenz-Zeiten

In TCP-Dialogen können Verzögerungen auftreten wie folgt:

- Tx-Host sendet Daten und TCP-PSH-Signal, Rx-Host sendet TCP-ACK-Empfangsbestätigung nicht sofort
- Tx-Host sendet Daten, Rx-Host sendet zwar TCP-ACK sofort, sendet aber die Antwort-Daten verzögert
- Tx-Host sendet Datenstoß über mehrere IP-Pakete verteilt, und zwischen diesen Paketen liegen Wartezeiten
- Tx-Host oder Rx-Host beenden die TCP-Session nicht sofort nach letzter Aktion (ggf Web-Proxy-Problem)

Alle (!) TCP-Pakete in allen (!) TCP-Sessions werden daraufhin analyisiert, welche Wartenzeiten der vier o.g. Latenz-Typen auftreten. Das Ergebnis ist eine exakte Statistik über alle (!) Wartezeiten innerhalb einer jeden (!) TCP-Session. Dies erlaubt genaue Aussagen darüber, warum "das Netzwerk langsam ist" bzw als langsam empfunden wird.

Diese TCP-Latenz-Statistiken können exakt aufzeigen,

- ob es der Client oder der Server ist, der lange Wartezeiten hat bis zur jeweiligen Antwort (ggf Überlastung)
- welche Subnetze an TCP-Sitzungen mit Wartezeiten beteiligt (ggf Hinweis auf Subnetz-Überlastung)

Die Statistiken weisen u.a. die auch die Gesamt-Dauer der TCP-Sitzung aus, das Rx/Tx-Datenvolumen, die schnellste und die langsamste Antwortzeit, etwaige Probleme mit der TCP Window Size (= Empfangspuffer) und/oder mit der Congestion Control.

Latenz-Zeiten werden zudem erfasst bei TCP-TLS-Sitzungsaufbau (Wartezeit beim TLS-Handshake).

Genauigkeit: 10^{-6} sec (= 0,000001 sec).

ICMP Latenz-Zeiten ("ping")

Das ICMP-Protokoll führt die "Ping"-Befehle aus und bewirkt die "Pong"-Antwort.
Die Analyse ermittelt für alle Ping-Pong-Dialoge die RTT = Round Trip Time (Antwortzeit).

Bei Dauer-Pings, die zu diesem Zwecke durchaus empfehlenswert sind, werden alle Ping-Pong-Ereignisse zeitlich analysiert und werden die Ergebnisse protokolliert. Dabei werden erfasst:

- kürzeste beobachtete Antwortzeit
- längste beobachtete Antwortzeit
- maximale errechnete Differenz-Zeit zwischen "schnell" und "langsam"
- mittlere errechnete Antwortzeit (statistisches Mittel)

Beim Vergleich der top langsamen Pong-Antworten und der jeweiligen IP-Adressen zeigt sich schnell, ob bestimmte IP-Subnetze bzw IP-Routen betroffen sind - oder eben nicht (was bedeutet, dass Verzögerungen nicht am IP-Übertragungsweg liegen, sondern zufällig an lokalen Gegebenheiten beim Ping-Empfänger = Pong-Sender).

Genauigkeit: 10^{-6} sec (= 0,000001 sec).

ICMP Meldungen

Im Falle von IPv4 werden alle, im Falle von IPv6 werden ausgewählte Meldungen und Nachrichten analysiert.

Hauptsächlich interessant sind Meldungen, die Fehler in der Verarbeitung und/oder Weiterleitung von IP-Paketen betreffen ("destination unreachable", "service unavailable"), aber auch Nachrichten, die sich auf Konfiguration und Administration von Endgeräten und Routern beziehen ("administratively prohibited", "address mask request").

ICMP Missbrauch

Sowohl ICMPv4 wie auch ICMPv6 können dazu gebraucht/missbraucht werden, das Netzwerk - in Grenzen - auszuspionieren bzw IP-Backholes ins Internet auszukundschaften.

Derlei Aktivitäten bzw die Bedingungen dazu werden von der Analyse gesondert erfasst und protokolliert.

SSL-TLS - Certificates & Encryption

Die Eröffnung verschlüsselter Transport-Kanäle mittels SSL bzw TLS wird genaustens analysiert.

Die umfangreichen TLS-Ergebnis-Tabellen weisen aus:

- alle Rechner, die als Sender oder Empfänger SSL/TLS verwenden
- alle SSL/TLS-Versionen pro SSL/TLS-Teilnehmer samt der Unterscheidung zwischen veraltet und aktuell
- Überprüfung der Zertifikat-Angaben bzw der Zertifikat-Gültigkeit, darunter das Ablauf-Datum
- Überprüfung ggf leichtfertig angebotener Zertifikate ohne Übereinstimmung von Host/Domain-Name(n)
- Überprüfung, ob nach erfolgtem Handshake die TLS-Session leer bleibt, also keine Daten liefen
- Überprüfung, ob die TLS-Session mit Applikations-Abbruch endet

HTTP Analyse

- Liste der angeforderten URL je Client / je Server
- Liste der je Client abgegebenen CONNECT-Befehle (HTTPS mit SSL/TLS)
- Liste der eingebetteten <iframe> Befehle und etwaiger Probleme, Prüfung enthaltener IP-Adressen und URL
- Liste der folgenden HTTP Header-Tags: X-Forwarded-For, Via, Content-Type, Content-Length, User-Agent
- Liste angesprochener IP-Adressen, die nicht zuvor per DNS aufgelöst wurden (hard coded, Sicherheitsproblem)

Die Liste der User-Agents (z.B. MS-IE, MS-Edge, MS-CryptoAPI, Mozilla, Safari, Zoom, Java, Guzzle, Feedly) gibt schnell Hinweise auf unerwünschte Endgeräte bzw unerwünschte Browser, die ggf gegen geltende Betriebs-Richtlinien von Anwendern installiert wurden - wobei die Nachricht ggf darin liegt, dass es überhaupt möglich war, dass ein Anwender installieren konnte (Admin-Rechte).

Auffallend große Download-Dateien, etwa: ISO-Images, fallen in der entsprechenden Liste schnell ins Auge.

HTTP-Anfrage, die nicht erfolgreich beantwortet werden, werden schnell sichtbar. Eine spezielle HTTP/HTML-Analyse-Funktion nachverfolgt die gesamten Sitzungsverläufe einschließlich der Bewertung der Aktionen.

Die Befehle GET, HEAD, POST, CONNECT werden im Besonderen beobachtet.

CONNECT-Befehle dienen dazu, verschlüsselte HTTPS-Verbindungen aufzubauen; hier kommt dann die o.g. TLS-Analyse zum Tragen.

Domain Services

Protokolle, über die Domains gebildet und verwaltet/konfiguriert werden, sind besonders Gegenstand der Analyse.

Dazu zählen u.a. ICMP, BOOTP/DHCP, NetBIOS, WINS, DNS, LDAP, KERBEROS, NTP, u.a.m.

- Liste aller ICMP-Anfragen/Antworten, die darauf abzielen, außerhalb der Domain-Verwaltung unterwegs zu sein
- Liste aller DHCP Clients samt wichtiger DHCP-Parameter, die von DHCP-Servern publiziert werden (IPv4+IPv6)
- Liste aller NetBIOS-Teilnehmer (veraltet, Sicherheits-Problem)
- Liste aller DNS/WINS-Anfragen und -Antworten samt Status (Erfolg/Fehler)
- Liste aller DNS-Anfragen, die im Verdacht stehen, problematische Internet-Temp-Domains anzusprechen
- Liste aller KERBEROS-Fehler/Ablehnungen, abgestuft in Grad der Schwere des Problems
- Liste aller KERBEROS/LDAP/DNS-Teilnehmer (Client-Server-Beziehungen)
- Liste aller LDAP-Realm-Client/Server
- Liste aller LDAP-Elemente/Objekte, die Identitäten im Active Directory abbilden (z.B. Login-Namen)
- Liste aller Windows-DFS-Referrals (Distributed File System) und Windows-Server-Shares

Sowohl die Event-Log-Ausgabe sowie die Listen und Tabellen sollen den Analysten in die Lage versetzen, die tatsächlichen Ist-Abläufe mit den Soll-Vorgaben abzugleichen.

In migrationsfreudigen Umgebungen kommt es schnell dazu, dass nicht alle Rechner beim jeweils letzten Migrationsschritt "mitgenommen" wurden; veraltete Server, die längst abgebaut hätten werden sollen, sind ggf immer noch aktiv (ohne dass es jemand bemerken würde); Fallback-Verhaltensweisen sind ggf immer noch aktiv, die abgestellt werden sollten (Sicherheits-Problem).

Insbesondere Windows-Logon mit NTLM und erfolgreiche Anmeldungen trotz KERBEROS-Ablehnung sind Hinweise auf unerwünschte Fallback-Verhaltensweisen, bei denen nicht die jeweils aktuelle/sichere Login-Variante zur Anwendung kommt, sondern auf frühere/unsichere Varianten zurück gegriffen wird. Derlei gehört unterbunden.

SNMP Management

Alle SNMP-Übertragungen werden analysiert, um zu prüfen, ob das SNMP-Management sicher ist (Passworte, Verschlüsselung) und erfolgreich ist (gegenseitige Erreichbarkeit der Clients und Server). SNMP-Daten, die der Identifizierung von Kommunikationsgeräten dienen, werden von der Analyse ausgelesen und in Listen ausgegeben.

- Liste aller SNMP-Zugriffe, die mit den Standard-Passworten "public" bzw "private" stattfinden (Sicherheit!)
- Liste aller SNMP-Zugriffe, die unverschlüsselt stattfinden
- Liste aller SNMP-Devices bzw der via SNMP übermittelten IP-Adressen, Standort-Daten, Namen
- Liste aller SNMP-Trap-Meldungen, die ihren Empfänger nicht erreichen, da sie geblockt/verworfen werden

Zur Erkennung technischer Fehler sowie zur Abwehr von Gefahren gehört unbedingt, dass das Meldewesen funktioniert, und SNMP-Trap-Meldungen gehören klar dazu. Trap-Meldungen, die an falsche = veraltete IP-Adressen gesendet werden, kommen nie an, entsprechend werden die Inhalte niemals und nirgends zur Kenntnis genommen.

Weiterhin gehören gut gepflegte Datenbanken zur wirkungsvollen Verwaltung eines Netzwerkes.

SNMP ist zwar nur eines der Mittel der Wahl, aber immer noch verbreitet und immer noch wirkungsvoll.

Entsprechend wird in der Analyse vermerkt, wenn SNMP-Get-Request/Reply nicht ankommen bzw wenn SNMP-Trap-Meldungen ins Nirgendwo geschickt oder im Übertragungsweg oder vom Empfänger geblockt werden.

Das Auslesen der SNMP-Device-Daten wird in Listen (s.o.) ausgegeben.

Die Analyse ist bestrebt, Management-Information eigenständig aus der 24/7/365-Beobachtung zu gewinnen, um offline wie online unabhängig zu sein von anderen Daten-Quellen - die zudem unzuverlässig sein können (s.o.).

SYSLOG Meldungen

Alle SYSLOG-Meldungen werden analysiert (nicht nur auf Standard-Port 514; auch auf abweichenden Ports).

Die Bedeutsamkeit/Dringlichkeit der mitgeteilten Sachverhalte wird dargestellt bzw untersucht. Bei bestimmten Meldungen wird aus den darin enthaltenen Angaben das voran gegangene Ereignis rekonstruiert und als eigenständiges Ereignis ins Event-Log geschrieben.

Beispiel: Eine Firewall meldet, dass ein bestimmter Verbindungsversuch geblockt wurde. Das Ereignis des Verbindungsversuchs selbst ist am MessPunkt nicht in den Trace-Daten enthalten, da der Verkehrsweg des Ereignisses nicht am aktuellen Analyse-Agenten vorbei führt. Aus der Firewall-SYSLOG-Meldung wird das Ereignis rekonstruiert und als Pseudo-Ereignis ins Analyse-Event-Log geschrieben, um die Lesbarkeit zu erleichtern und das nachgehende, automatische Filtern nach bestimmten Ereignissen zu unterstützen.

Da in SYSLOG-Meldungen nicht nur MAC-Adressen und IP-Adressen genannt werden, sondern oft auch DNS-Namen, FQDN, Benutzer-Namen, Login-Namen, werden diese Angaben ebenfalls ausgelesen und verarbeitet.

Eine Liste von Schlüssel-Begriffen (trigger terms) wird verwendet, um SYSLOG-Meldungen zu markieren.

Weiterhin können spezielle Filter gesetzt werden, um besonders bedeutsame Sachverhalten in Report-Listen zu erfassen, etwa: Meldungen über Strom-Schwankungen an Switch-Ports etc etc.

E-Mail

Alle E-Mail-Server werden erfasst und gelistet. Bei unverschlüsselten Mail-Verbindungen werden die Handshakes und die beteiligten IP-Adressen im Event-Log ausgegeben. Unverschlüsselte Inhalte werden **nicht** betrachtet.

Oracle / SQL

- SQL-Status-Codes bzw Fehler-Codes werden ausgelesen samt ggf vorhandener Fehler-Beschreibungen.
- SQL-Benutzer-Namen (MySQL) werden ausgelesen und gelistet.

Voice over IP (VoIP) / SIP / Real Time Protocols

- Real Time Protocols werden analysiert: Dienste für Data-Streaming, Video, Telefonie
- SIP: die Betriebs-Parameter aller SIP-Teilnehmer werden erfasst und in Listen ausgegeben (SIP Options)

Die Liste der SIP Options gestattet das Erkennen von Konfigurations-Fehlern und ggf Sicherheits-Problemen wie beispielsweise unerwünschten Teilnehmern und/oder Betriebs-Parametern. Erfasst/gelistet werden:

- SIP-Versionen
- IP-Adressen
- Telefon-Nummern
- Mail-Adressen
- Device Description (Server-Namen, Geräte-Bezeichnungen)
- Transport-Protokoll: UDP oder TCP / Port-Nummer

Im Zusammenhang mit der Liste der SIP-Teilnehmer und SIP-Options steht ggf die Liste der STUN-Aktivitäten, da VoIP-Sessions die freie Durchleitung der Daten bei Firewalls und Routern verlangt; diese Freischaltung des Verbindungsweges über das Internet und durch die angeschlossenen Unternehmensnetze läuft über das STUN-Protokoll (siehe oben).

MS Windows

- Liste aller Windows Clients, Server, User Names, Shares, DFS Referrals (Distributed File System)
- Liste aller gescheiterten Zugriffsversuche (ggf Sicherheits-Problem, da Angriff möglich)
- Liste aller Zugriffe auf unerwünschte Verzeichnisse, etwa ..\Adobe\Flash\ .. (Sicherheits-Problem)
- Liste aller Versuche, Logon mittels NTLM durchzuführen (veraltet, ggf Sicherheits-Problem)
- Event Log: Darstellung der Aktionen: Server Login, Share Connect, Verzeichnis-/Datei-Zugriffe, etc.

Analyse-Ergebnisse: Tages-Reports, Monats-Reports, Aggregierung, Filterungen, Weiterleitungen

Jeder Analyse-Agent erzeugt pro Tag einen umfassenden Report, indem die gewonnenen Erkenntnisse in Listen und Tabellen abgelegt werden, teilweise lesbar in .TXT Dateien, teils maschinenlesbar im .CSV Format (Excel).

Ein HTML-Interface kann genutzt werden, um die Tagesberichte von außen abzufragen (Download).

Interessanter ist das Sammeln, Aggregieren und Filtern der Berichtsdateien auf der zentralen Sammel-Station.

Jeder Analyse-Agent legt die Tages-Reports unter Tagesdatum ab. Auf dem Sammel-Rechner könne dann mit dort arbeitender Spezial-Softwarwe z.B. die Tabellen aller KERBEROS-Ticket-Ablehnungen oder die Listen aller Benutzer-/Login-Namen aggregiert und sortiert werden.

Dieses Aggregieren und Sortieren kann netzwerkweit pro Tag oder Monat durchgeführt werden.

Auf diese Weise können aus den Listen+Tabellen tages-aktuelle Gesamt-Übersichten automatisch erzeugt werden.

Um Zusammenhänge sichtbar zu machen, die sich durch Listen nicht erzeugen lassen, läuft auf dem Sammel-PC dauerhaft 24/7/365 eine spezielle Filter-Engine, die Event-Log-Meldungen durchmustert, die via Syslog von den Analyse-Agenten gesendet wurden.

Spezial-Filter können veranlassen, dass bestimmte Syslog-Meldungen bzw Filter-Ergebnisse automatisch weiter

geleitet werden, wahlweise erneut per Syslog und/oder per E-Mail (verschlüsselt oder Klartext); es können im Falle von Syslog mehrere IP-Adressen zur Weiterleitung hinterlegt werden, bei E-Mail mehrere Empfänger-Adressen.

Die Filter-Bibliotheken können jederzeit den Bedürfnissen bzw den lokalen Gegebenheiten angepasst werden.

Mehrere Millionen Ereignis-Meldungen pro Tag sind je nach Einzelfall ggf problemlos filterbar.

Bei sehr großen Datenmengen kann es sein, dass die Filter-Engine nicht täglich die gesamte Menge der per Syslog eingetroffenen Meldungen verarbeiten kann. In diesem Falle gibt es zwei Möglichkeiten:

- Verzicht, täglich 100% der Meldungen zu filtern; es wird nur jeder zweite oder dritte Tag gefiltert
- Verminderung der Zahl der aktiven Event-Log-Filter; kann ggf zu partieller Blindheit führen
- Verteilung der eintreffenden Syslog-Meldungen auf mehrere Server, dadurch wieder 100% verarbeitet

Ergebnis der Filterung sind thematisch eingegrenzte Filter-Event-Logs, pro Filter abgelegt in jeweils einem eigenen Verzeichnis auf der Festplatte.

Weiterhin führt die Filter-Engine eine Treffer-Tabelle, die für jeden Filter ausweist, wann gefiltert wurde, mit welchem Packet-Timestamp das gesuchte Ereignis zuletzt als Treffer gefunden wurde, wann die Filter-Definition angelegt wurde, wann zuletzt die Filter-Definition geändert wurde.

Diese Treffer-Tabelle ist eine leicht lesbare Quelle Erkenntnis.

Das selbe gilt für die aggregierten Ergebnis-Listen, bei denen die Ergebnisse aller Analyse-Agenten auf dem zentralen Sammel-PC zusammen gezogen und sortiert/priorisiert werden.

Daten-Vertraulichkeit: Bei *Synapse Managed Services* per Fernzugriff verbleiben die Daten sämtlich auf den Datenträgern des Kunden, nur die Video-Daten verlassen den Herrschaftsbereich des Kunden. Es gibt daher auch kein DSGVO-Problem, da es keine Datenverarbeitung durch Dritte bzw Weitergabe an Dritte gibt.