SYNAPSE: ANALYSE

MERKMALE - LEISTUNGEFÄHIGKEIT - EXPERTISE

- Synapse Networks GmbH ist nach eigener Kenntnis das **einzige Unternehmen** in Deutschland, das **ausschließlich LAN-WAN-Analyse** betreibt. Dadurch ist Synapse voll fokussiert und, mangels jeglicher Verpflichtung gegenüber IT-Herstellern und IT-Dienstleistern, **frei von jeglichem Interessenskonflikt**.

  Synapse betreibt LAN-Analyse seit 1991 und ausschließlich seit 2000.

- Synapse wird geführt von **Senior Analyst Frank R. Walther**, in der LAN-Analyse tätig seit 1991, seit 1996 Autor der Synapse-Analyse-Experten-Systeme und damit vermutlich **der dienstälteste LAN-Analyst Deutschlands**. Er hat zudem in den Jahren 2000-2003 als erster Autor die in Deutschland Grund legende **Fachliteratur zur LAN-WAN-Analyse** veröffentlicht (*Networker's Guide; Registry Guide; jeweils bei: Markt+Technik bzw Pearson*).

  Anmerkung(1): Im Jahr 2002 gab es Verhandlungen mit Hewlett-Packard. HP wollte damals die Synapse-Analyse-Software auf die HP High-End Analyse-Systeme portieren. Der Handel kam damals nicht zu Stande, weil HP die Voraussetzungen auf Hardware- und Organisations-Ebene nicht schaffen konnte.

  Anmerkung(2): Im Jahr 2007 wurde das Synapse-Analyse-Experten-System von der Loseblatt-Sammlung „LAN-Analyse & Troubleshooting" (WEKA/Interest-Verlag) wie folgt bewertet: „Das momentan am Markt beste Expertensystem nach Meinung des Autors ist das relativ unbekannte TraceMagic."

- Synapse verwendet zur automatisierten Analyse (das ist: die selbsttätige Auswertung von Messdaten mit der Zielsetzung des Auffindens von Fehlern und Sicherheitsgefahren) **ausschließlich eigene Software**, die seit 1996 kontinuierlich entwickelt wird. Mit einer Reaktionszeit, die regelmäßig wenige Tage beträgt, kann neuartigen Fehlern, die bislang nicht bekannt waren, mit neu programmiertem Software-Code begegnet werden. Damit können die am Markt typischen Wartezeiten auf Updates von Protokoll-Decodern unterboten werden.

- Synapse-Analyse ist **non-invasiv**. Die Erfassung der Messdaten erfolgt über Switch-Mirror-Ports, die zwar Kommunikationsdaten zum Analyse-System ausgeben, vom Analyse-System aber keine Datenpakete annehmen bzw nicht ins Netzwerk des Kunden weiter geben. - Somit ist die Synapse-Analyse **frei von jeglicher Einwirkung**. **Es bedarf daher auch keiner Vorab-Prüfung**, ob die Analyse ihrerseits ein Problem oder gar Sicherheits-Risiko sein könnte.

Synapse Networks GmbH – www.synalyst.net – www.synapse.de

Peter-Bischof-Str. 2a 0700.SYNAPSE.**C** [**C**]all www.synapse.de
55435 Gau-Algesheim 0700.SYNAPSE.**F** [**F**]ax office-contact@synapse.de

Handelsregister: Amtsgericht Mainz HRB 43073 / USt-ID: DE226433719

- Synapse-Software kann zeitlich unbegrenzt (fast) beliebige Datenmengen verarbeiten, und dies bei **Online- und Offline-Analyse**, nur begrenzt durch die technischen Grenzen des Computersystems, auf dem die Software läuft.

- Synapse-Software kann sowohl bei Online-Analyse wie auch bei nachträglicher Offline-Analyse die binären LAN-Pakete der an einer Störung beteiligten Maschinen und Prozesse heraus filtern (**Binär-Filter**). Dies ist grundlegend für die forensische Qualität der Analyse (**gerichtsfeste Beweissicherung**).

- Synapse-Software enthält u.a. eine nachgelagerte **Filter-Engine**, die Ereignis-Meldungen der Analyse-Agenten, die beim zentralen **Syslog-Sammler** erfasst und gespeichert werden, permanent durchmustern und priorisieren.

Praxis-Beispiel (Synapse-Referenz-Kunde):

- Im September 2018 gehen pro Tag regelmäßig 20-30 Mio Ereignis-Meldungen an der zentralen Sammel-Station (Syslog-Sammler) ein.

  Die dortige Synapse-*Filter-Engine* enthält z.Zt. **ca 600 Filter-Definitionen**, von denen **ca 400 aktiv** sind; diese Filter bilden nicht nur aktuelle Fehler ab, sondern auch behobene Fehler der Vergangenheit; so kann überprüft werden, ob bereits behobene Fehler weiterhin und dauerhaft abwesend bleiben (= **Verifikation** des dauerhaften Abhilfe-Erfolgs; Nachweis der dauerhaften **Abwesenheit** früherer Fehler).´

Synapse Analyse Experten System:

- Die in der *Filter-Engine* hinterlegten Filter-Definitionen bilden die **umgebungsspezifischen Fehler und Verdachtsfälle** ab; sie erfassen nicht nur statische Merkmale wie etwa Adressen oder Namen, sondern auch (und insbesondere) variable Ereignisse und Szenarien, was zum Aufdecken insbesondere von Sicherheits-Risiken unabdingbar ist.

- Synapse-Analyse erfasst automatisch **fehlschlagende bzw erfolglose Versuche** von Netzwerk-Komponenten, **Verbindung aufzunehmen** zu anderen Komponenten/Teilnehmern; diese Fehlversuche werden protokolliert und teils in chronologischen Event-Logs, teils in gegliederten Tabellen ausgegeben, die ihrerseits in Tagesberichten abgelegt werden. Dies erlaubt das **Erkennen illegaler bzw gefährlicher Aktivitäten** im Netzwerk.

  Dazu gehören u.a. (Auswahl; Liste ist notwendig unvollständig):

Unbekannte Broadcasts; unverschlüsselte oder ungesicherte SNMP-Management-Meldungen; unbeantwortete oder abgewiesene TCP-Sitzungsversuche; angenommene, aber datenlose TCP-Sitzungen (Pseudo-Verbindungen ohne jeglichen Austausch von Daten); unbeantwortete „Ping"-Rufe; abgewiesene Windows-Logon/Connect-Versuche; Versuche, Verbindungen direkt bzw über illegale/heimliche Proxy-Server ins Internet aufzunehmen (statt via Proxy-Server bzw DMZ); durch Router/Firewalls blockierte Verbindungs-versuche, wobei zusätzlich ermittelt bzw dargestellt wird, ob die vergeblich angesprochene IP-Adresse bereits zuvor im Netzwerk aktiv war (was auf technischen Fehler hinweist) – oder eben nicht (was auf illegale Aktivität hinweist); ob HTTP-Zugriffe direkt auf IP-Adressen stattfinden (statt auf DNS-Namen), was u.U. ebenfalls auf **illegale Aktivitäten** hinweisen kann.

- Synapse-Analyse erfasst Ereignisse, die auf **wechselnde Wege** der Pakete von Teilnehmer-A zu Teilnehmer-B schließen lassen (Wechsel der Zahl der Router-Querungen; Wechsel des Routers bzw Router-Interfaces im lokalen Netzwerk-Segment des Messpunktes). Dies gibt nicht nur Hinweise auf etwaige technische Fehler, sondern auch **Hinweise auf etwaige Intercept-Angriffe / Man-In-The-Middle-Attacks**.

- Synapse-Analyse erfasst **sicherheitsrelevante Vorgänge**, sowohl offensichtliche (z.B. abgelaufene Passworte, abgelehnte Logins) wie auch verborgene (Rechner versuchen im Hintergrund, entgegen der vorgesehenen Policy zu kommunizieren). Sobald ein Rechner mit einem Sicherheits-Problem auffällig wird, kann durch **Filter** auch das weitere Kommunikationsverhalten der betreffenden Maschine erfasst und protokolliert, können **Zusammenhänge und Muster** erkannt und bewiesen werden. Es kann sofort untersucht werden, ob auch andere Maschinen das erkannte Verhalten zeigen, bzw welche Maschinen mit einander das Verhalten teilen. Versuche, die gewollten/geplanten Strukturen zu unterlaufen, werden erkannt und protokolliert, ebenso das Ergebnis (ob die Versuche erfolgreich waren/sind oder nicht).

- Synapse-Analyse ist darauf gerichtet, dem Kunden schnellstmöglich Ergebnisse zu liefern, die ihn befähigen, Änderungen vorzunehmen zu dem **Zweck, die Angriffsfläche seiner Systeme zu klein wie möglich zu halten**. Dies richtet sich auch – und insbesondere – auf die Management-Systeme.

- Synapse-Analyse erfasst dauerhaft die wesentlichen **Identitäts-Merkmale** der kommunizierenden Teilnehmer (MAC-Adressen, IP-Adressen, NetBIOS-Namen, WINS-Namen, DNS-Namen, DHCP-Client-Adressen, DHCP-Client-Namen, DHCP-Vendor-ID) sowie etwaige **Wechsel bzw Änderungen** dieser Identitäts-Merkmale und ihrer etwaigen Kombinationen. Auf den Analyse-Agenten sowie auf der Zentral-Konsole (Syslog-Sammler) wird jeweils eine entsprechende **Host-ID-Datenbank** geführt, die abfragbar ist auf einzelne Host-ID-Merkmale (Include/Exclude-Filter) bzw auf etwaige Host-ID-Wechsel und Zeitpunkte; im Falle des Verdachts auf ID-Wechsel können automatische Benachrichtigungen erfolgen.

Diese Host-ID-Datenbanken werden sowohl auf den Analyse-Agenten wie auch an der zentralen Sammel-Station endlos fortlaufend geführt und reichen bei o.g. **Referenz-Kunden** bereits (je nach Messpunkt) mehrere Jahre zurück. Somit kann im Verdachtsfall schnell ermittelt werden, wann und wo bestimmte ID-Merkmale (Adressen, Namen) erstmals auftraten und wann Änderungen derselben erfasst wurden.

- Synapse-Analyse protokolliert alle diese **Ereignisse in indizierter Form**, was besagt, dass das jeweils zugehörige originale=binäre LAN-Paket bei Bedarf sofort manuell aus den **Messdaten im Ring-Buffer** heraus gegriffen werden kann (Index: Datei-Nummer / Paket-Nummer).

- Synapse-Analyse untersucht auch die **Performance der beteiligten Clients und Server** auf TCP-Dialog-Ebene mit gesonderten Schwerpunkten auf **Verzögerung, Wartezeit, Timeout**. Für jede einzelne (!) TCP-Sitzung werden u.a. erfasst: Sitzungsdauer; Datenmenge; Datendurchsatz, pro Sekunde gemittelt; Router-Hops; TCP-Window-Size-Probleme (low/zero); Zahl der fehlenden/verlorenen TCP-Pakete; Zahl der Wiederholungs-Übertragungen; Art der Sitzungs-Beendigung (geregelt=Handshake oder ungeregelt=Abbruch); Verzögerungen und Wartezeiten wie folgt: (**1**) zwischen Daten-Zustellung durch den Sender und darauf folgender Quittung/Bestätigung durch den Empfänger; (**2**) zwischen Eingang der Partner-Quittung des Empfängers und der nächsten Übertragung des Senders; (**3**) zwischen zwei TCP-Paketen des selben Daten-Stoßes (bis zum TCP-PSH); (**4**) zwischen dem letzten Payload-Packet (Paket mit Nutzdaten) und dem Handshake zur Beendigung der Sitzung (Timeout-Szenario). Es kann präzise ermittelt und nachgewiesen werden, welcher Art die Verzögerungen sind, welche TCP-Sitzungen „langsam" machen, bzw auf welche(n) Wartezeit-Typ(en) die tatsächlichen Verzögerungen zurück gehen.

- Für alle **PING-Anfragen** werden, sofern es PONG-Antworten gibt, für alle Host-zu-Host-Paarungen die Antwortzeiten ermittelt (**RTT: Round-Trip-Time**), wobei gesondert erfasst werden: (**1**) kürzeste aller RTT zwischen A und B; (**2**) längste aller RTT zwischen A und B; (**3**) durchschnittliche RTT; (**4**) zeitliche Differenz (Delta-Zeit) zwischen kürzester und längster RTT; (**5**) Zahl der Router-Hops zwischen A und B. Auf diese Weise lässt sich präzise erkennen und nachweisen, ob bzw dass es Schwankungen gibt in der Qualität von Verbindungen insbesondere zwischen Standorten, die via WAN/Internet verbunden sind.

- Synapse-Analyse weist darüber hinaus auf allen Netzwerk-Ebenen **die Quellen von „langsamen" Zugriffen** bzw Zugriffsversuchen nach, wie etwa: Routing-Probleme, DNS-Probleme (Namensauflösung kann nicht geliefert werden oder dauert zu lang); Berechtigungsprobleme (falsche Auth-Data und/oder Fall-Back-Abläufe); Überlast-Blockierungen (meistens bei Servern oder Routern); auffällige oder fehlerhaftes Network-Congestion-Management (IP/TCP); Hop-to-Hop-Probleme im WLAN; Active/Passive-Interface-Probleme bei HSRP-Failover-Strecken; und anderes mehr.

- Synapse-Analyse hat somit **forensische Qualität**: Allen erfassten und protokollierten Ereignissen stehen die originalen, binären Messdaten gegenüber (sofern im so genannten Ring-Buffer noch vorhanden, was wiederum korreliert mit Festplatten-Kapazität und Datendurchsatz).

- Synapse-Analyse gibt **Alarm, wenn kritische Ereignisse** erkannt werden:

  Die verteilt im Netzwerk arbeitenden Analyse-Agenten können auf erkannte Ereignisse mit Meldungen via **Syslog und/oder E-Mail** reagieren. Es können jeweils mehrere Empfänger für Syslog und/oder E-Mail hinterlegt werden. Bei fehlerspezifischen Analyse-Filtern, die vom Anwender/Administrator gesetzt werden, können für verschiedene Filter jeweils getrennt Empfänger-Listen für die E-Mail-Benachrichtigungen hinterlegt werden.

  Dadurch werden die richtigen Techniker/Administratoren adressiert.

  Die Filter-Engine, die beim zentralen Syslog-Symmler arbeitet, kann über E-Mail ebenfalls Benachrichtigungen an hinterlegte Empfänger versenden.

  Die Inhalte der E-Mails werden in verschlüsselten Anhang-Dateien versendet.

- Synapse-Alarm-Meldungen via E-Mail sind also **nicht für Unbefugte lesbar**.

- Synapse-Berichte werden bei den Analyse-Agenten in **Tages-Reports** abgelegt; die beim Syslog-Sammler arbeitende Filter-Engine legt Ergebnis-Berichte je Filter-Lauf ab.

Synapse-Analyse **zeigt** nicht (nur), was sein *könnte* – sondern *tatsächlich*, **was ist**.

SMART NETWORK ANALYSIS

https://www.synalyst.net/

(Stand: 2018-09-13)

Synapse Networks GmbH – www.synalyst.net – www.synapse.de

Peter-Bischof-Str. 2a 0700.SYNAPSE.**C** [**C**]all www.synapse.de
55435 Gau-Algesheim 0700.SYNAPSE.**F** [**F**]ax office-contact@synapse.de

Handelsregister: Amtsgericht Mainz HRB 43073 / USt-ID: DE226433719