synalyst

SMART NETWORK ANALYSIS

24/7 IT-Security

Monitoring + Analysis

5 Beispiele aus der Praxis: Sicherheitsprobleme bei Kunden im Umfeld von Finanzwirtschaft, NATO und Bundesregierung

Synapse Networks GmbH
Peter-Bischof-Straße 2a
55435 Gau-Algesheim
www.synalyst.net
it-security@synalyst.net
0 67 25 999 07 10

Sicherheit durch LAN/WAN-Analyse

Nur die ständige Analyse des LAN-WAN Datenverkehrs offenbart Gefahren für Betrieb und Sicherheit und erlaubt vorbeugendes Handeln.

synalyst liefert das Campus- und weltweit arbeitende Analyse-Experten-System sowie auf Wunsch den Managed Service

Nur SIEM allein ist auch keine Lösung

Viele Unternehmen vertrauen auf SIEM-Lösungen.

Das ist einerseits richtig: Das Aggregieren aller Ereignis-Meldungen ist von großem Vorteil.

Andererseits kann jedes SIEM nur sammeln und auswerten, was es auch geliefert bekommt:

Wenn aktive Komponenten über Ereignisse und Fehler keine Meldung machen (heißt: nichts ins Event-Log schreiben, keine Syslog-Meldung ans SIEM senden), ist das SIEM zwangsläufig blind.

Ebenso zwangsläufig bleiben dann ausgerechnet die kritischsten Vorfälle unterhalb des Radarschirms: unsichtbar.

Die folgenden Beispiele beweisen es…

5 Beispiele aus der Praxis

Die folgenden Beispiele stammen aus Unternehmen bzw. Einrichtungen mit höchsten Anforderungen an Verfügbarkeit und Sicherheit ihrer IT aus folgenden Bereichen:

- Finanzwirtschaft
- NATO / Militärisch-industrieller Komplex
- weltweites LAN/WAN im Regierungsumfeld

Beispiel 1
Firewall schickt interne Daten ins Internet

Die Internet-Firewall wurde erneuert bzw ausgetauscht gegen das neueste und leistungsfähigste Modell des Herstellers.

Die **synalyst** Analyse jedoch offenbarte:

Interne Daten flossen ab ins Internet. Der Firewall-Admin überprüfte die Konfiguration und befand, dass die Firewall auf »BLOCKING« gestellt sei. Da der Befund aber zweifelsfrei war, wurde der Hersteller angesprochen. Die Antwort kam binnen 24 Stunden:

Das neue Modell war nicht ausreichend getestet worden. Ein Entwickler hatte in der Beschriftung des GUI-Schalters leider »OPEN« und »CLOSED/BLOCKING« vertauscht.

Wer also »BLOCKING« anklickte, bewirkte im Hintergrund »OPEN«.

Da die Firewall schlicht den gegebenen Befehlen gehorchte, sah sie ihr eigenes Verhalten nicht als Fehler an und gab folglich auch keine Meldung ab: nicht ins interne Event Log, nicht per Syslog an den SIEM-Server.

Nur die synalyst Echtzeit-/Nahzeit-Analyse bewahrte den Kunden vor einer Katastrophe.

Beispiel 2
Core-Switch kopiert Daten und verbreitet sie

Zwei Fehler überlagerten sich und führten in den nahezu völligen Verlust der Datenvertraulichkeit:

Ein aus zwei Instanzen bestehender virtueller Switch (zwei physikalische Einheiten verhalten sich, als wären sie eine) wurde auf Redundanz konfiguriert, wobei im Normalbetrieb jeder Switch für jeweils einen der zwei Gebäudeteile zuständig war. Fiel einer der beiden Switche aus, würde der andere übernehmen.

Dabei unterlief dem Techniker der Fehler, dass er die Rx/Tx-Interfaces des sog. Trunk-Links (der die beiden Einheiten verbindet) identisch bezeichnete; der zweite Fehler war, dass der Switch dies tatsächlich zuließ und nicht abwehrte (was zwingend hätte sein müssen).

In der Folge wurden alle Ethernet-Pakete des einen Switches in Kopie über den Trunk zum jeweils anderen Switch gesendet. Da dort jedoch die Empfänger-Ethernet-Adresse zwangsläufig unbekannt war, wurden gemäß IEEE-Standard-Vorschrift alle Ethernet-Pakete auf alle LAN-Segmente verteilt.

So wurden z. B. E-Mails, die an den Vorstand gerichtet waren, im jeweils anderen Gebäudeteil auf allein Leitungen per Kopie verteilt.

Wo immer eine USB-Buchse an jeglichem Client-PC offen war (nicht blockiert war) und wer-auch-immer einen Portable Wireshark vom USB-Stick startete, konnte ALLES mitlesen.

Da der Switch selbst keinen Fehler darin erkannte, gab er keine Fehler-Meldungen ab.

Nur die synalyst Echtzeit-/Nahzeit-Analyse bewahrte den Kunden vor einer Katastrophe.

Beispiel 3
Defekt in der Load-Balancer-Redundanz

Die zwei Interfaces eines Load Balancers, die gegenseitig auf Redundanz eingestellt waren, verloren nach einem Software-Update die Fähigkeit, sich zu synchronisieren, weil sie die Heartbeat-Meldungen, die sie sich gegenseitig zusandten, nicht mehr akzeptierten.

Beide Load-Balancer-Interfaces sandten sich zwar Meldungen über die Nicht-Annahme der Heartbeat-Packets zu, schrieben aber keine Meldung in ihr internes Event Log und sandten auch keine Meldung via Syslog ans SIEM.

Wäre nun eine der beiden Load-Balancer-Einheiten ausgefallen, hätte die jeweils andere Einheit dies nicht registriert und hätte folglich auch nicht für den anderen den Betrieb übernommen. Eine schwere Störung des Betriebs wäre die unweigerliche Folge gewesen.

Mangels Meldung blieb auch diese Störung vollständig unter dem Radarschirm des Kunden.

Besonder bitter: Dem Hersteller war dieser Fehler bekannt – ohne jedoch seinen Kunden darüber Mitteilung gemacht zu machen.

Nur die synalyst Echtzeit-/Nahzeit-Analyse bewahrte den Kunden vor einer Katastrophe.

Beispiel 4
Firewall lässt ungebetene Gäste ins Netz

Vor Jahren war einmal für eine begrenzte Zeit den Mitarbeitern externer Partner-Unternehmen der Zugriff auf bestimmte interne Server gestattet worden.

Leider jedoch hatte der Firewall-Admin vergessen, das Firewall-Tor wieder zu schließen.

Es zeigte sich, dass von externen Rechnern immer noch Zugriffe stattfanden.

Die Firewall konnte darin keine Gefahr sehen, weil dies ihrer Konfiguration entsprach.

Auch diese Sicherheitsverletzung blieb daher vollständig unterhalb des Radar-Schirms, und auch die SIEM-Instanzen waren daher blind.

Nur die synalyst Echtzeit-/Nahzeit-Analyse bewahrte den Kunden vor einer Katastrophe.

Beispiel 5
DNS-Server sprechen untrusted DNS an

Aus Sicherheitsgründen sollten die Campus-DNS-Server ihre DNS-Anfragen nur an solche Internet-DNS-Server weiter leiten, die als vertrauenswürdig zugelassen sind.

Durch einen Konfigurationsfehler jedoch wurden DNS-Anfragen, die wegen verspätet eintreffender Antworten ins Timeout liefen, über das offene/ungeschützte Gäste-WLAN an völlig beliebige und daher ggf. auch nicht-vertrauenswürdige DNS-Server weiter geleitet.

Unmittelbare Gefahr daraus: Spoofing-Angriffe.

Auch hier gab es im SIEM des Kunden keine Meldung, da die DNS-Server keinen Fehler erkannten: es entsprach ihrer Konfiguration.

Nur die synalyst Echtzeit-/Nahzeit-Analyse bewahrte den Kunden vor einer Katastrophe..

Sprechen Sie uns an
www.synalyst.net
it-security@synalyst.net
0 67 25 9 99 07 10
Ihr Partner in Deutschland und weltweit