ABGEGRENZTE DIAGNOSE

Ein Problem. Drei Stunden. Ein klarer Befund.

Sie haben ein technisches Problem, das Ihr Team schon Zeit gekostet hat. Ich untersuche genau dieses Problem, zum Festpreis, und Sie bekommen einen schriftlichen Befund, mit dem Sie entscheiden können.

290 € netto

Festpreis für bis zu drei Stunden, einschließlich Auswertung und Übergabe. Sie sprechen direkt mit mir, Leon Ostendorf, IT Architect für Global Core Infrastructure, und ich mache die Arbeit selbst. Überwiegend remote, zu vereinbarten Terminen.

So läuft die Diagnose

01 · KOSTENLOS

Passung klären

Bis 15 Minuten, schriftlich oder im Gespräch. Ich sage Ihnen ehrlich, ob das Problem zu mir passt. Eine technische Untersuchung findet hier noch nicht statt.

02

Auftrag festhalten

Ein Problem, das gewünschte Ergebnis, die betroffenen Systeme und klare Grenzen. Schriftlich, bevor die Arbeit beginnt.

03

Daten bereitstellen

Exporte, Protokolle oder Konfigurationen, die wir vorher benennen. Zugänge nur wenn nötig, zeitlich begrenzt und nach Ihrer Freigabe. Passwörter nie per E-Mail.

04

Untersuchen

Bis zu drei Stunden. Reicht die Zeit nicht, bekommen Sie den belegten Stand und eine Einschätzung, was noch fehlt. Mehr Zeit gibt es nur nach Ihrer Zustimmung.

05

Übergabe

Ein Bericht wie im Muster auf den nächsten Seiten, auf Wunsch kurz besprochen. Jeder Befund ist als bestätigt, plausibel oder offen markiert.

06 · IHRE ENTSCHEIDUNG

Nächster Schritt

Die Umsetzung kann Ihr Team selbst übernehmen. Oder ich biete sie an: 95 € netto pro Stunde, mit fester Kostenobergrenze.

Typische Anlässe

- Anmeldeprobleme im Netz: Netzwerkzugangskontrolle, VPN, WLAN
- Störungen nach Updates in VMware-Umgebungen
- Monitoring meldet zu viel oder das Falsche
- Backups laufen, aber niemand weiß, ob der Restore klappt

Was die Diagnose nicht ist

- Keine garantierte Fehlerbehebung in drei Stunden
- Keine unbegrenzte Recherche
- Kein Betriebsvertrag und keine Bereitschaft
- Keine Änderungen an produktiven Systemen ohne Ihre Freigabe

Fiktives Beispiel. Firma, Umgebung und Zahlen sind erfunden. Der Bericht zeigt Aufbau und Tiefe einer Diagnose und ist keine Kundenreferenz.

01 · ERGEBNIS AUF EINEN BLICK

Warum landen seit Montag einzelne Windows-Clients im Gast-VLAN?

Auftraggeber: ein Systemhaus, das einen Logistikbetrieb mit zwei Standorten und rund 180 Arbeitsplätzen betreut. Betroffen sind kabelgebundene Arbeitsplätze mit 802.1X-Anmeldung.

> **Der RADIUS-Server sendet nach dem Zertifikatswechsel nur sein eigenes Zertifikat, ohne Zwischenzertifikat. Clients, die das neue Zwischenzertifikat noch nicht kennen, brechen die Anmeldung ab und landen im Gast-VLAN.**

21 von 176	BESTÄTIGT	**2,5 h**	**ca. 2 h**
Clients betroffen, rund 12 %	Ursache am Testclient nachgestellt	von 3 h Diagnose genutzt	geschätzte Umsetzung

Wirkung im Betrieb

Betroffene Mitarbeiter haben nur Internet, aber keinen Zugriff auf ERP und Dateiserver. Seit Montag sind dazu rund 20 Tickets eingegangen. Die Zahl steigt, weil Notebooks nach und nach ins Büro zurückkommen.

Warum gerade diese Clients

Vor der Anmeldung hat ein Client noch kein Netz und kann das fehlende Zwischenzertifikat nicht nachladen. Es fehlt vor allem auf Notebooks, die seit dem Wechsel keine aktuelle Gruppenrichtlinie bekommen haben.

Empfehlung

1 SOFORT
Zwischenzertifikat in die Kette des RADIUS-Dienstes aufnehmen. Danach sendet der Server die vollständige Kette, und alle Clients können sie prüfen, ohne dass an den Geräten etwas geändert wird.

2 DIESE WOCHE
Zwischenzertifikat zusätzlich per Gruppenrichtlinie verteilen. Das sichert auch Geräte ab, die später andere Dienste mit derselben Kette nutzen.

3 DAUERHAFT
Checkliste für den nächsten Zertifikatswechsel und eine Ablaufwarnung 30 Tage vorher im Monitoring.

ANGEBOT FÜR DEN NÄCHSTEN SCHRITT, OPTIONAL

Umsetzung der Punkte 1 bis 3 gemeinsam mit Ihrem Administrator, in einem vereinbarten Zeitfenster und mit gesichertem Rückweg. Bei 75 % des Budgets gibt es einen Zwischenstand.

max. 285 €
netto · geschätzt 2 h, Obergrenze 3 h zu 95 €

02 · AUFTRAG UND GRENZEN

Was untersucht wurde und was nicht

PUNKT	VEREINBART
Frage	Warum werden einzelne Windows-Clients an kabelgebundenen Ports seit Montag ins Gast-VLAN gelegt?
Im Auftrag	RADIUS-Server, zwei Access-Switches als Stichprobe, drei Windows-Clients
Nicht im Auftrag	WLAN, Prüfung der gesamten internen PKI, Änderungen an produktiven Systemen
Zugang	Begleitete Bildschirmsitzung mit dem Administrator des Systemhauses, 60 Minuten. Sonst nur bereitgestellte Exporte, keine eigenen Zugangsdaten.
Ergebnis	Schriftlicher Befund mit Nachweisen und Empfehlung, kurze Übergabe per Telefon

03 · DATENBASIS

Jede Aussage lässt sich auf eine Quelle zurückführen

QUELLE	WOFÜR GENUTZT	AUSSAGEKRAFT
RADIUS-Protokoll, Export über drei Tage	Abbrüche je Client, Zeitpunkt und Switchport	HOCH
Portkonfiguration der zwei Switches, Auszug	Regel, die bei fehlgeschlagener Anmeldung ins Gast-VLAN legt	HOCH
Ereignisprotokolle von drei Clients, zwei davon betroffen	Abbruchgrund auf der Clientseite	HOCH
Serverzertifikat und gesendete Kette	Aussteller, Gültigkeit, Anzahl der Zertifikatsstufen	HOCH
Gruppenrichtlinie für das 802.1X-Profil	Vertrauenswürdige Zertifizierungsstellen, Verteilung	MITTEL

04 · VORGEHEN

Fünf Schritte, 2,5 Stunden

NR.	SCHRITT	ZEIT
1	Auftrag und Daten sichten, Hypothesen festhalten	0,5 h
2	RADIUS-Protokoll auswerten: Abbrüche nach Client, Uhrzeit und Port	0,5 h
3	Betroffene und nicht betroffene Clients vergleichen: Zertifikatsspeicher, Profil, Ereignisprotokoll	0,5 h
4	Gesendete Kette prüfen und Ursache am Testclient nachstellen, in der begleiteten Sitzung	0,5 h
5	Bericht schreiben und übergeben	0,5 h
	Summe	**2,5 h**

05 · BEFUNDE MIT NACHWEIS

Was belegt ist, was plausibel ist, was offen bleibt

NR.	BEFUND	NACHWEIS	STAND
B1	Die 21 betroffenen Clients brechen die Anmeldung bei der Prüfung des Serverzertifikats ab. Keine Richtlinie lehnt sie ab.	RADIUS-Protokoll zeigt Sitzungen ohne Abschluss statt Ablehnungen. Die Ereignisprotokolle beider betroffener Clients nennen ein nicht vertrauenswürdiges Serverzertifikat.	BESTÄTIGT
B2	Der Server sendet seit dem Wechsel nur eine Zertifikatsstufe, ohne Zwischenzertifikat.	Mitschnitt der Anmeldung am Testclient: eine Stufe statt zwei.	BESTÄTIGT
B3	Das neue Serverzertifikat stammt von einem neuen Zwischenzertifikat. Nicht betroffene Clients haben es bereits, betroffene nicht.	Zertifikatsspeicher der drei Clients verglichen.	BESTÄTIGT
B4	Betroffen sind überwiegend Notebooks, die seit dem Wechsel keine aktuelle Gruppenrichtlinie bekommen haben.	Für 15 der 21 Geräte über den Zeitpunkt der letzten Richtlinienaktualisierung belegt, für 6 nicht geprüft.	PLAUSIBEL
B5	Ob das WLAN dasselbe Problem hat.	Nicht untersucht, außerhalb des Auftrags.	OFFEN

Nachgestellt am Testclient

Mit Freigabe des Administrators wurde das Zwischenzertifikat auf einem Testclient entfernt: Anmeldung scheitert, Gast-VLAN. Nach dem erneuten Import: Anmeldung klappt, Produktions-VLAN. Damit ist die Ursache belegt und nicht nur vermutet.

Ausgeschlossen

- Switches: Firmware und Portkonfiguration seit Juli unverändert, nicht betroffene Clients funktionieren an denselben Ports.
- Uhrzeit: auf allen drei Clients korrekt.
- Ablauf: Serverzertifikat gültig bis 2028.

LESEHILFE

BESTÄTIGT durch Nachweis belegt. PLAUSIBEL gut begründet, aber nicht vollständig belegt. OFFEN nicht untersucht oder nicht klärbar mit den vorhandenen Daten. Eine Ursache wird nie als bewiesen dargestellt, solange sie nur vermutet ist.

06 · UMSETZUNG, FALLS GEWÜNSCHT

Woran wir erkennen, dass es behoben ist

Prüfkriterien

- Zwei bisher betroffene Notebooks melden sich am Port an und landen im Produktions-VLAN.
- Der Mitschnitt am Testclient zeigt zwei Zertifikatsstufen.
- Das RADIUS-Protokoll zeigt 24 Stunden lang keine abgebrochenen Sitzungen dieser Art.

Rückweg

Die bisherige Zertifikatskonfiguration des RADIUS-Dienstes wird vorher gesichert und lässt sich in wenigen Minuten wiederherstellen. Die Änderung erfolgt in einem vereinbarten Zeitfenster, der Administrator gibt sie frei.

07 · ABSCHLUSS DER DIAGNOSE

Aufwand, Zugänge, Daten

Tatsächlicher Aufwand	2,5 Stunden von 3 Stunden. Abgerechnet wird der Festpreis von 290 € netto.
Zugänge	Keine eingerichtet. Die begleitete Sitzung ist beendet.
Bereitgestellte Daten	Werden nach der vereinbarten Frist gelöscht. Im Bericht stehen nur Auszüge, die für den Nachweis nötig sind.
Änderungen	Nur am Testclient, mit Freigabe und wieder zurückgestellt. An produktiven Systemen wurde nichts verändert.
Offene Punkte	B4 für 6 Geräte prüfen. B5 klären, falls auch im WLAN Störungen gemeldet werden.

Ihr Problem ist ein anderes?

Beschreiben Sie es in ein paar Sätzen an contact@alveqio-infrastructure.com oder über das Formular auf alveqio-infrastructure.com. Ich melde mich mit einer ehrlichen Einschätzung, ob eine Diagnose sinnvoll ist. Die Klärung bis 15 Minuten kostet nichts.

Leon Ostendorf · IT Architect für Global Core Infrastructure