



Logging und Monitoring

Ein weiterer Schritt zu mehr Sicherheit

Sowohl im BDEW-Whitepaper als auch als Folge der ISMS-Zertifizierung sind **Betreiber kritischer Infrastrukturen** dazu angehalten, ihre Systeme und Geräte **besser zu schützen und zu kontrollieren**. Wir bieten Ihnen aus diesem Grund zwei neue Services an: Logging Ihrer Geräte und Monitoring Ihrer Systeme.

Monitoring und Logging sind **nicht beschränkt** auf Ihre leittechnischen Systeme, sondern lassen sich **auf die gesamte IT-Infrastruktur** ausweiten. Mit Hilfe beider Systeme können Anomalien und Angriffe analysiert werden. Sie sind damit wichtige Werkzeuge beim **Aufdecken von Sicherheitslücken** und unterstützen Sie dabei, **für die Zukunft gerüstet** zu sein.

Was ist Logging?

Fast alle Geräte in einem Netzwerk legen Log-Files an, die verschiedene Informationen speichern. Diese sind allerdings begrenzt und oft nur wenige Minuten verfügbar.

Typische Log-Informationen sind:

- An-/Abmeldungen, Anmeldeversuche
- Konfigurationsänderungen
- Fehlgeschlagene Zugriffe
- VPN-Verbindungen
- Fehlermeldungen

Logging-Systeme können diese Geräte-Informationen **zentral und über einen längeren Zeitraum speichern**. Diese können Sie dann **später auswerten**. Sowohl im BDEW-Whitepaper (Kapitel 4.5.6) als auch in der Norm ISO 27001 (Kapitel 12.4) wird Logging als Sicherheitsmaßnahme gefordert.

Mit diesen Informationen sind Sie besser auf zukünftige Angriffe und Angriffsversuche vorbereitet.

Was ist Monitoring?

Ein Monitoring-Tool kann durch stetiges Beobachten von bestimmten Parametern eines Systems erkennen, wann diese nicht mehr der Norm oder den Vorgaben entsprechen.

Typische Parameter sind:

- CPU-Temperatur
- Prozessorlast
- Festplatten-Füllstand / Festplattenfehler
- Aktive Betriebszeiten
- Verfügbarkeit von Diensten

Das Monitoring-Tool überwacht Ihre Systeme kontinuierlich hinsichtlich der korrekten Funktionalität und **löst im Falle einer Störung einen Alarm** aus. Erwähnung findet das Thema in der Norm ISO 27001 (Kapitel 4.4.1).

Mit diesen Informationen erhalten Sie mehr Kenntnisse über Ihre Systeme und können diese weiter optimieren.

- ✓ Wenig Aufwand – viel Nutzen
- ✓ Sicherheitsnachweis gemäß BDEW-Whitepaper und ISO 27002
- ✓ Überprüfung Ihrer IT-Verfügbarkeit und IT-Stabilität (24/7)
- ✓ Frühzeitiges Erkennen kritischer Betriebszustände



Logging: Unser Angebot für Sie

Im Bereich Logging setzen wir auf ProLog der Firma NETZWERK Software GmbH.

Schritt 1: Software

Sie erhalten von uns die benötigte Software-Lizenz.

Schritt 2: Vorbereitung & Spezifikation

Wir legen gemeinsam mit Ihnen fest: Die zu überwachenden Geräte und Ereignisse, Aufbewahrungsdauer und Zugriffsberechtigungen, Transport der Daten zum Log-Server. Mit diesen Vorgaben erstellen wir das Protokollierungskonzept.

Schritt 3: Inbetriebnahme

In einer virtuellen Umgebung, Registrierung, Einrichtung des Loggings auf Firewall etc., Einweisung der Anwender

Bei Bedarf bieten wir Ihnen auch zeitliche oder ereignisorientierte Auswertungen als Dienstleistung an.

[Sprechen Sie uns an!](#)



Monitoring: Unser Angebot für Sie

Im Bereich Monitoring setzen wir auf Paessler PRTG Network Monitor.

Schritt 1: Software

Sie erhalten von uns die benötigte Software-Lizenz.

Schritt 2: Vorbereitung & Spezifikation

Wir legen gemeinsam mit Ihnen fest: Die zu überwachenden Geräte und Ereignisse, Alarmierung bei Störungen, Transport der Daten

Schritt 3: Inbetriebnahme

Auf einem eigenständigen Windows-Server, Registrierung, Einrichtung der Server, Domänen-Controller und Arbeitsplätze, Einweisung der Anwender

Bei Bedarf bieten wir Ihnen zeitliche oder ereignisorientierte Anpassungen der Auswertung und Alarmierung als Dienstleistung an.

[Sprechen Sie uns an!](#)