

PRESSEMITTEILUNG

TeleTrust-Podcast: Intrusion Detection

Berlin, 13.10.2026 - Wie lassen sich Angreifer möglichst frühzeitig erkennen? Und woran lässt sich feststellen, dass sich jemand unbefugt in einem Netzwerk bewegt? Mit diesen Fragen beschäftigt sich der aktuelle TeleTrust-Podcast. Carsten Vossel (CCVOSEL) spricht mit Tobias Schlattmann (Cybersense) über Intrusion Detection und die Frage, wie Unternehmen verdächtige Aktivitäten erkennen können, bevor ein Angriff größeren Schaden verursacht.

<https://www.teletrust.de/podcasts/>

Im Gespräch geht es unter anderem darum, wie sich Angreifer nach einem initialen Zugriff in einer fremden IT-Umgebung orientieren und welche Spuren sie dabei hinterlassen. Tobias Schlattmann erläutert, welche Rolle Netzwerk- und Portscans sowie Abfragen des Active Directory spielen und warum gerade diese frühen Aktivitäten für die Angriffserkennung interessant sind. Auch die zunehmende Bedeutung von Künstlicher Intelligenz bei der Beschleunigung solcher Aktivitäten wird thematisiert.

Ein weiterer Schwerpunkt ist die Unterscheidung zwischen relevanten Warnungen und Fehlalarmen. Unter dem Stichwort "Alert Fatigue" wird erläutert, welche Herausforderungen eine große Zahl von Alarmmeldungen für Security-Analysten mit sich bringt und wie Deception-Ansätze dabei helfen können, eindeutige Signale für verdächtige Aktivitäten zu erzeugen.

Darüber hinaus beleuchtet die Folge, wie Sensorik im Netzwerk funktioniert, welche Bedeutung der Überwachung von Netzwerkverkehr und Active Directory zukommt und was nach einer erkannten Attacke passiert. Dabei geht es auch um die Frage, wann eine automatisierte Reaktion sinnvoll ist und wann der Mensch die letzte Entscheidung treffen sollte.

Tobias Schlattmann macht dabei deutlich, warum es bei der Angriffserkennung vor allem auf den Zeitpunkt ankommt: Nicht erst dann reagieren, wenn ein Angreifer sein eigentliches Ziel erreicht hat, sondern möglichst früh erkennen, wie er sich im Netzwerk orientiert und seinen Weg aufbaut. Dabei werden auch die Überwachung von IT- und OT-Umgebungen sowie die Auswahl besonders relevanter Netzwerkbereiche für die Überwachung angesprochen.

Der Podcast gibt Einblicke in aktuelle Ansätze der Angriffserkennung und zeigt, welche Bedeutung eine frühzeitige Detektion für die Reaktionsfähigkeit von Unternehmen haben kann.

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Der Bundesverband IT-Sicherheit e.V. (TeleTrust) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breitgefächerte Mitgliedschaft und die Partnerorganisationen verkörpert TeleTrust den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrust bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrust ist Träger der "TeleTrust European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrust Information Security Professional" (T.I.S.P.) und "TeleTrust Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrust ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.