DIE WICHTIGKEIT VON NETZWERKMONITORING, ANALYSE UND ANGRIFFSERKENNUNG

MARKTBETRACHTUNG

Kosten reduzieren und Betriebssicherheit erhöhen

Notfallvorsorge, Security Management, Angriffserkennung, sichere Vernetzung in Industrie 4.0 Projekten und Instandhaltungskosten: In all diesen Bereichen lässt sich mit Netzwerkmonitoring oder Network Traffic Analysis (NTA) Zeit und Geld sparen. Das Einsparpotential in Relation zur Investition ist groß. Das Ziel, Netzwerke und Produktionsanlagen zu schützen, ist effizient durch Netzwerkmonitoring und Analyse erreichbar.

Die Vielzahl der erfolgreichen Hackerangriffe und Erpressungen (Ransomware) der letzten Monate haben in der Forensik gezeigt, dass mit einem Netzwerkmonitoring ein Angriff bereits frühzeitig erkannt worden wäre. Ein rechtzeitiger Eingriff hätte das Schadensausmaß beträchtlich reduziert, in den meisten Fällen sogar verhindert.

Die Angriffserkennung (IDS – Intrusion Detection System) sollte das ordnungsgemäße Verhalten automatisiert lernen, wie es das IT-Sicherheitsgesetz 2.0 fordert. Mit der Deep Packet Inspection (DPI) werden alle Einzelheiten der Kommunikation bis in die Protokollebene aufgenommen. Die kontinuierliche Analyse (Anomalieerkennung) wird als die Methode der Angriffserkennung genutzt. Identifizierte Änderungen im Kommunikationsmuster der Anlage werden so als Folge eines Angriffs oder einer andersartigen Störung im Betrieb bewertet und daraufhin zielgerichtet alarmiert. Mit der Kombination dieser Funktionen werden neue und unbekannte Angriffe erkannt.

VIDEC.

Kosten reduzieren und Betriebssicherheit erhöhen

Fortsetzung von Seite 1

Eine permanente Pflege von Angriffsmustern wie bei herkömmlichen IDS ist nicht notwendig - das Einspielen von Updates, Signaturen oder Threat Intelligence Daten bekannter Schadsoftware entfällt. Damit läuft man den Angriffsmustern nicht mehr hinterher. Zusätzlich stehen für das Security Management und die Cybersecurity ein aktuelles Assetregister und ein Netzstrukturplan zur Verfügung. Dies ist die elementare Anforderung, um ein durchgehendes Schutzlevel mittels Risikoanalyse umzusetzen. Bei Industrie 4.0 Erweiterungen oder Retrofitting lassen sich mögliche Risiken sofort und schnell erkennen.

Das BSI liefert im Blatt CS 134 zu »Monitoring und Anomalieerkennung in Produktionsnetzwerken« detaillierte Beschreibungen zur Umsetzung von Netzwerkmonitoring und Analyse – für die Anforderungen des ITSiG 2.0 eine angemessene Risikovorsorge im Unternehmen.

Sie erhalten in der folgenden Marktbetrachtung* weitere Informationen zur Technologie, den Anforderungen und dem Status von Netzwerkmonitoring und Analyse.

Wenn Sie Unterstützung bei der Verwendung von Fachbegriffen benötigen, können Sie auf unserer Webseite im Glossar entsprechende Informationen abrufen.

Was ist Netzwerkmonitoring und Analyse?

Netzwerkmonitoring und Analyse ist eine wichtige Cybersecurity-Strategie, die die Suche nach Bedrohungen von Perimetern und Endpunkten auf Netzwerkverkehr verlagert. Sie nutzt eine Kombination aus maschinellem Lernen, fortschrittlicher Analytik und regelbasierter Erkennung. Mit dem erstellten Basismodell des normalen Netzwerkverhaltens können passende Warnungen generiert werden, die das System anhand abnormaler Muster erkennt.

Dieser Ansatz eignet sich gut für offene und sich verändernde Netzwerkumgebungen. Seine Effektivität liegt in der Identifizierung von schwer erkennbaren Bedrohungen.

In dieser Umfrage erfahren Sie mehr über das Bewusstsein, das Wissen und die Nutzung von Netzwerkmonitoring und Analysen durch Fachleute. Diese Spezialisten arbeiten im Umfeld der Cybersecurity von Unternehmen und in Security Operations Centern (SOC), die auch von Managed Security Service Providern betrieben werden.

Wir hoffen, dass Sie die geteilten Informationen als nützlich für die Beurteilung, Bewertung und Verfeinerung Ihrer eigenen Cybersecurity-Strategien empfinden.

Viel Spaß beim Lesen des Berichts.

KERNAUSSAGEN

Netzwerkmonitoring und DPI Integration wachsen immer schneller

Eine Mehrheit der Unternehmen (87 %) nutzt entweder bereits Netzwerkanalyse-Tools oder plant den Einsatz. Eine ähnliche Mehrheit (76 %) nutzt oder plant einen Invest in Deep Packet Inspection (DPI) zur Stärkung der eigenen Cybersecurity.

Netzverkehrsdaten sind von entscheidender Bedeutung

Nicht alle Befragten sind sich der zentralen Rolle der DPI Sensoren bei Netzwerklösungen bewusst. Für diejenigen, die damit vertraut sind (64%), sind die von den Sensoren gesammelten Daten von entscheidender Bedeutung. Sie halten sie sogar für wertvoller als Informationen aus anderen Quellen (z.B. Endpunkte, IDS-Warnungen und Protokolle).

Advanced Persistent Threats und Verschlüsselung sind die Top-Herausforderungen

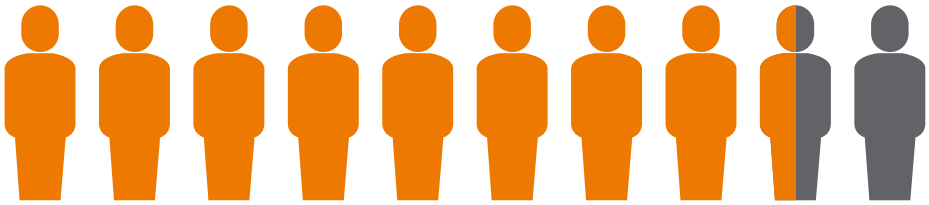
Mehr als die Hälfte der Befragten nennen die Wirksamkeit gegen Advanced Persistent Threats (APT) als die wichtigste Aufgabe von Netzwerkmonitoring und Analysen bei der Eindämmung von Cyber-Bedrohungen. Und 94 % der Befragten bezeichnen eine der wichtigsten DPI Sensorfunktionen als ein mäßig bis sehr dringendes Cybersecurity-Problem (die Einsicht in verschlüsselten Datenverkehr).

Weitere Antworten geben Aufschluss darüber, wie Cybersecurity-Experten DPI gestütztes Netzwerkmonitoring und Analysen einsetzen, um die Herausforderungen in Bezug auf Sichtbarkeit, Effizienz und Agilität anzugehen.

MARKTANALYSEN*

WIE GUT KENNEN SIE SICH MIT NETZWERKMONITORING UND ANALYSEN AUS?

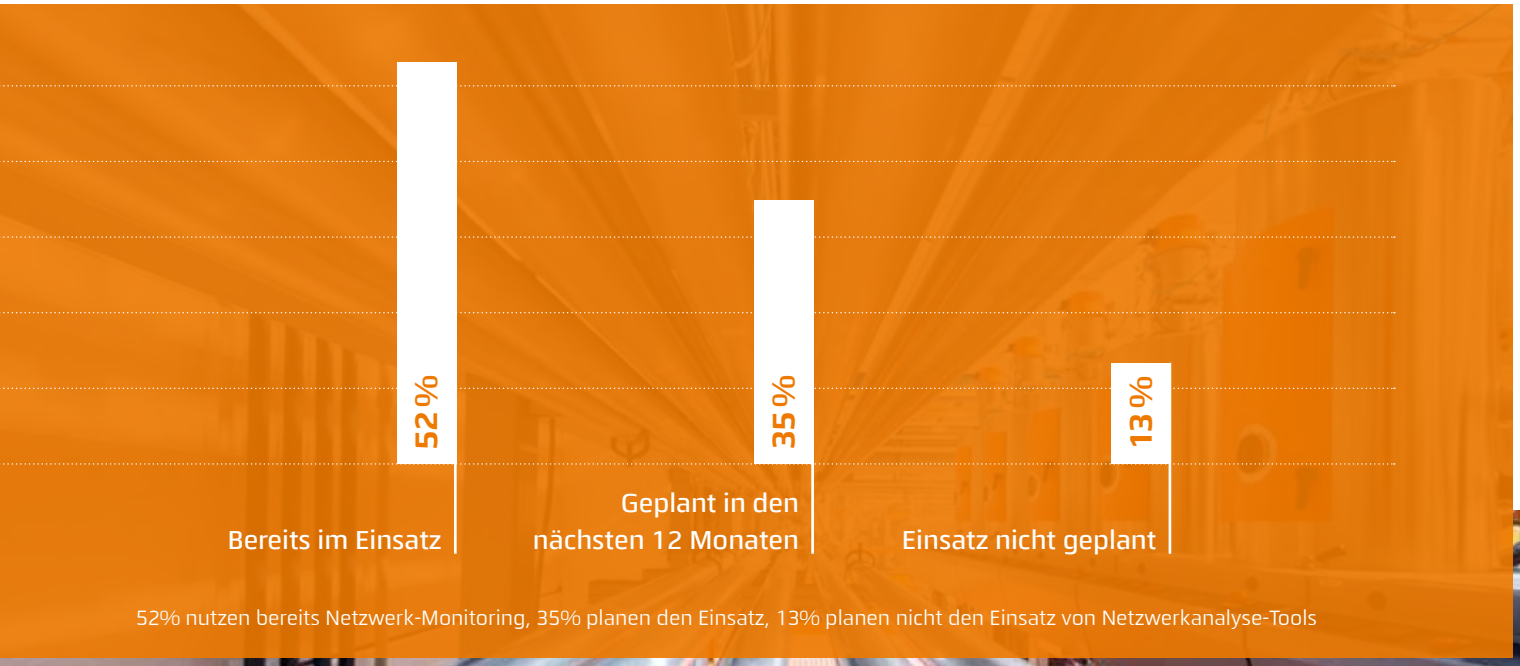
9 von 10 der Umfrageteilnehmer sagen aus, dass sie sich mit Netzwerkmonitoring und Analysen gut auskennen. Dies reflektiert ein wachsendes Verständnis bzgl. dieser Thematik im Gesamtmarkt. Sie stellt auch die Wichtigkeit bei der Gesamtbetrachtung der Sicherheit heraus.



87 von 100 Befragten berichten, dass sie sich mit Netzwerkmonitoring und Analysen auskennen

NUTZUNG VON NETZWERKMONITORING UND ANALYSEN

Die Mehrheit der Organisationen (52%) verwendet bereits Netzwerkanalyse-Tools oder plant den Einsatz dieser Technologie (35%). Unbeachtet bleiben die Funktion und Qualität des Netzwerkmonitorings, sowie die Verwendung der gewonnenen Daten und Informationen für weitere Betrachtungen im Bereich Security. In vielen Unternehmen wird das Netzwerk primär hinsichtlich der Funktion betrachtet und ausschließlich von der OT betreut.



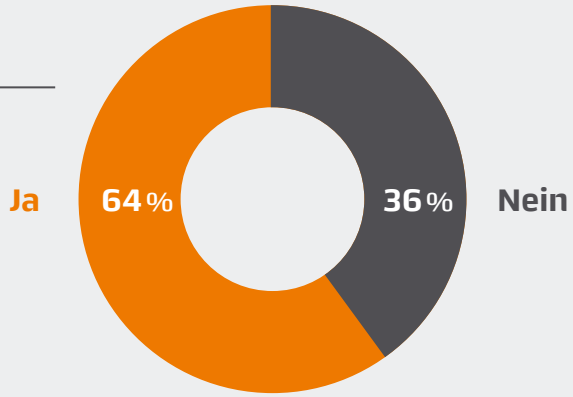
52% nutzen bereits Netzwerk-Monitoring, 35% planen den Einsatz, 13% planen nicht den Einsatz von Netzwerkanalyse-Tools

SIND SIE MIT DPI SENSOREN ODER DETEKTOREN VERTRAUT?

Deep Packet Inspection (DPI - Tiefgreifende Paket Inspektion) ist eine erweiterte Methode beim Netzwerkmonitoring und der Analyse. Sie identifiziert Protokolle und Anwendungen anhand der Auswertung. Wobei eine Kombination aus erweiterten Technologien angewendet wird - einschließlich zustandsabhängiger Inspektion, verhaltensabhängiger und statistischer Analysen und Heuristiken.

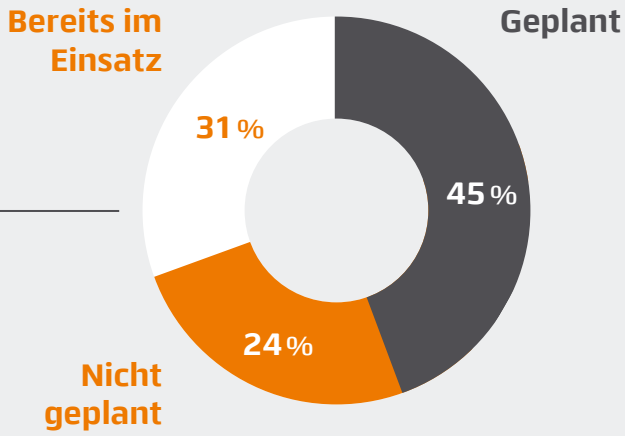
Netzwerkmonitoring mit DPI macht Datenkommunikationen bis zum Layer 7 vollumfänglich sichtbar. Dazu gehören Protokolldetails wie Dateitypen, Dateierweiterungen, Laufwerke sowie Funktionsaufrufe und Parameter in Automatisierungsprotokollen.

Bei der Frage nach Bekanntheit von DPI Sensoren oder Detektoren haben fast zwei Drittel (64%) der Befragten ausgesagt, sie würden sich mit dieser Materie auskennen. Für 36% ist dieses Thema neu.



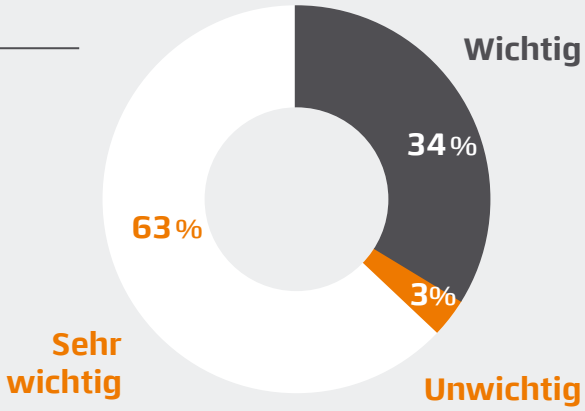
VERWENDEN SIE DPI SENSOREN ZUR ABWEHR GEGEN CYBERANGRIFFE?

Eine große Anzahl der Unternehmen (31%) verwendet bereits DPI Sensoren. Sie dienen vollumfänglich der Erhöhung der Cybersicherheit. Weitere 45% planen, diese Technologie kurzfristig einzusetzen. 24% der Befragten konnten dazu noch keine Aussage treffen.



DER WERT VON NETZWERKDATEN

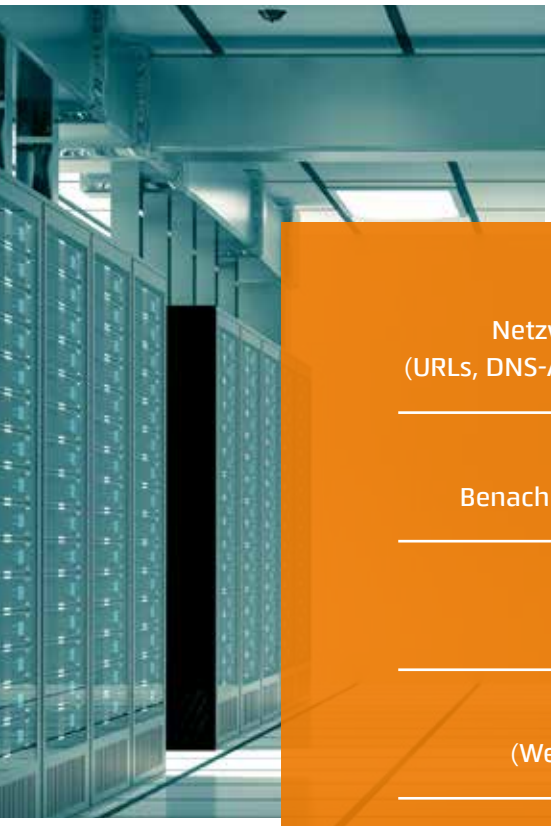
Eine Mehrheit von 63% der IT-Security Fachleute sagt aus, dass Netzverkehrsinformationen ermittelt durch DPI Sensoren von entscheidender Bedeutung seien. Weitere 34% halten es zumindest für wichtig. Eine eindeutige und entscheidende Aussage über diese Daten und Informationen.

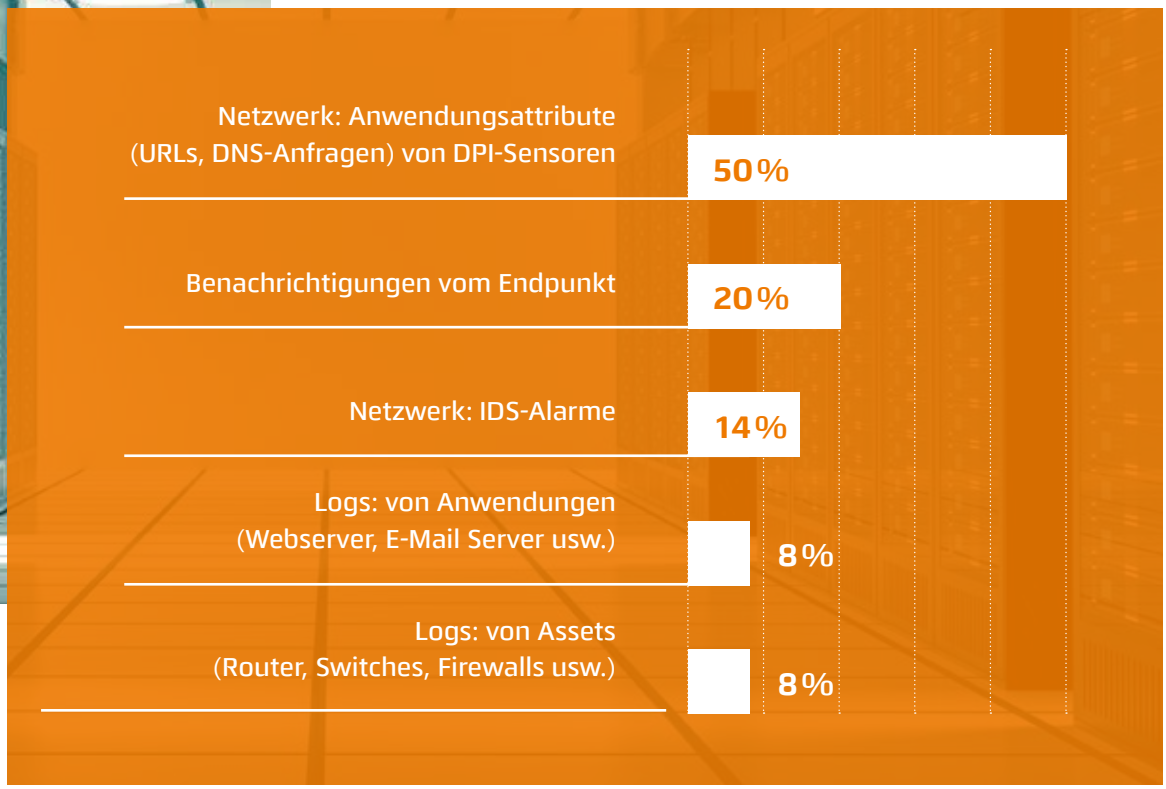


*Original erschienen von Cybersecurity Insiders Holger Schulze, CEO and Founder sponsored by ENEA Qosmos Division 2019

WELCHE INFORMATIONSQUELLEN SIND IHRER MEINUNG NACH AM EFFEKTIVSTEN FÜR DIE CYBERSICHERHEIT?

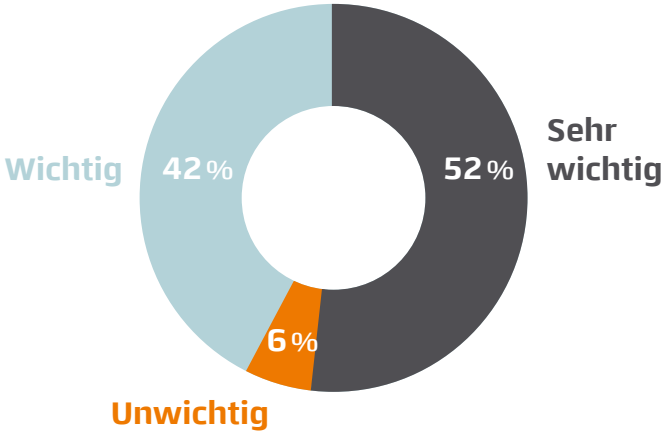
Bei der Netzwerkanalyse bevorzugen IT-Sicherheitsfachleute Analysen, die Anwendungsattribute wie z.B. URLs und DNS-Anfragen von DPI Sensoren enthalten, vor anderen Quellen wie Benachrichtigungen vom Endpunkt oder IDS-Alarme.





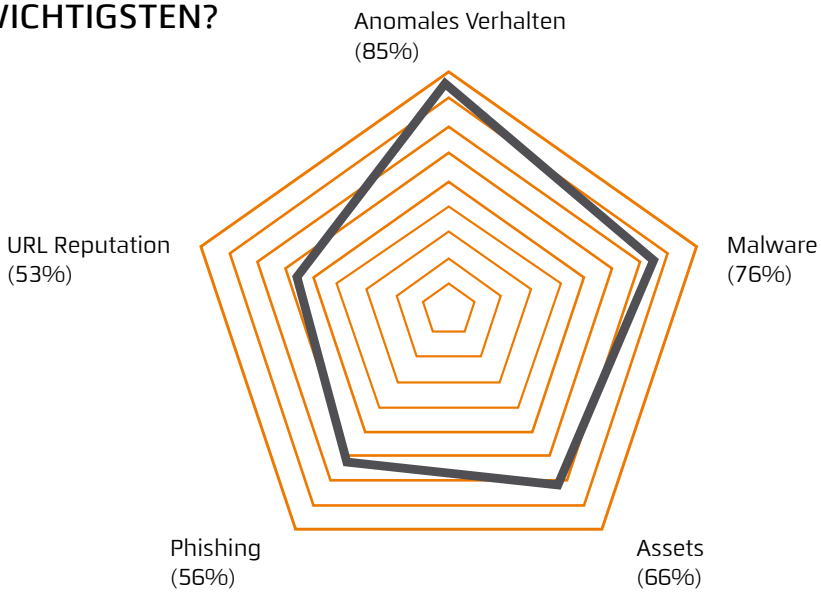
WIE WICHTIG IST ES, TIEFERE EINSICHT IN DEN VERSCHLÜSSELTEN DATENVERKEHR IHRES NETZWERKS ZU ERHALTEN?

Über 52% der Befragten betrachten es als sehr wichtig, tiefere Einsicht in den verschlüsselten Datenverkehr zu erhalten. Weitere 42% sagen, es sei wichtig. Lediglich 6% der IT-Sicherheitsfachleute betrachten dies als unwichtig. Auch hier ein klares Statement zur Transparenz im Datenverkehr.



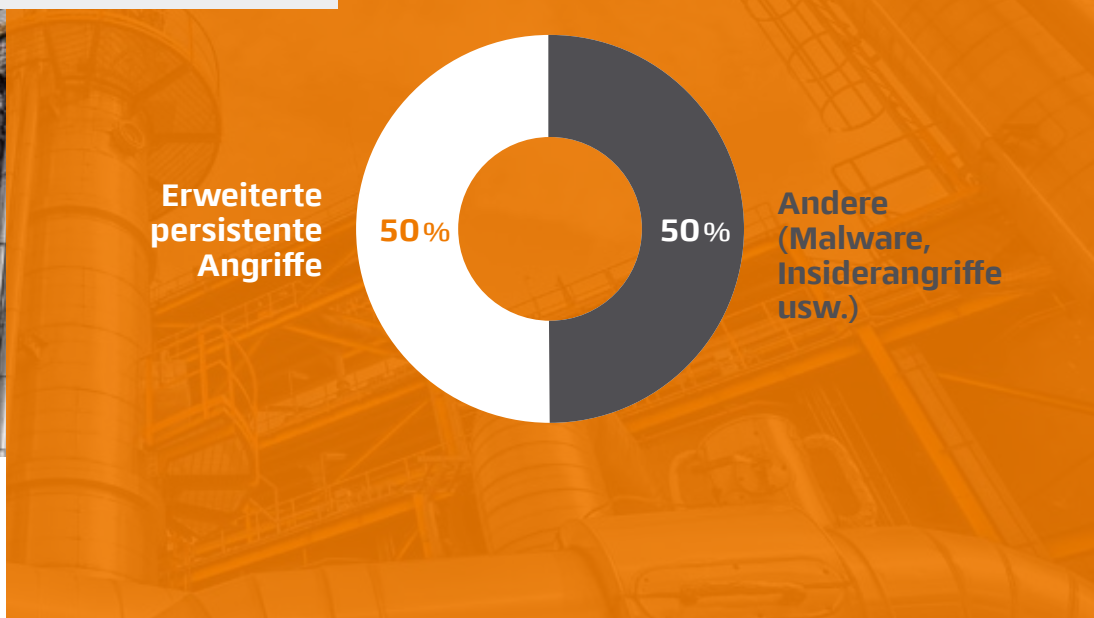
WELCHE ANWENDUNG SEHEN SIE ALS TEIL DER NETZWERKANALYSE AM WICHTIGSTEN?

Wenn nach der wichtigsten Anwendung zur Netzwerkanalyse gefragt wird, bewerten IT-Sicherheitsfachleute die Erkennung anomalen Verhaltens mit 85% am höchsten, gefolgt von Malwareerkennung mit 76% und Geräteerkennung mit 66%.



WELCHER CYBERANGRIFF WIRD VON DPI AM BESTEN ABGEWEHRT?

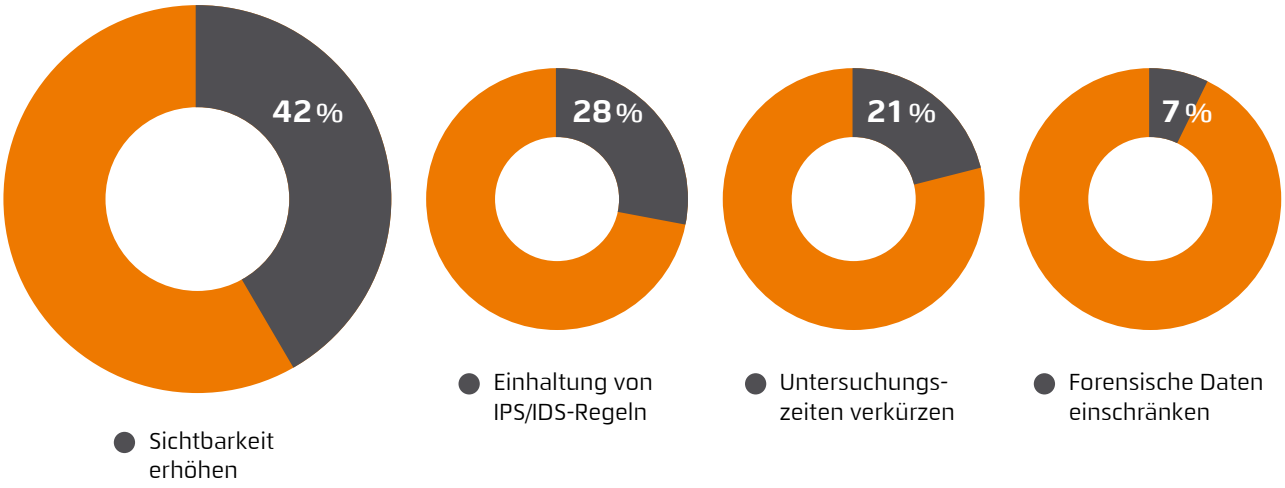
DPI kann nahezu jeder Organisation helfen, gezielte Cyberangriffe abzuwehren. Die Befragten wurden gebeten, Angriffsarten in Bezug auf den Abwehreinfluss von DPI von 1 bis 5 zu bewerten. Mehr als die Hälfte gab Advanced Persistent Threats (Erweiterte persistente Angriffe) die höchste Bewertung. Andere Angriffsarten, welche von DPI abgewehrt werden können, sind bekannte und unbekannte Schadsoftware sowie Insider-Angriffe (ebenfalls 50%).



WARUM WÜRDEN SIE DPI SENSOREN EINSETZEN?

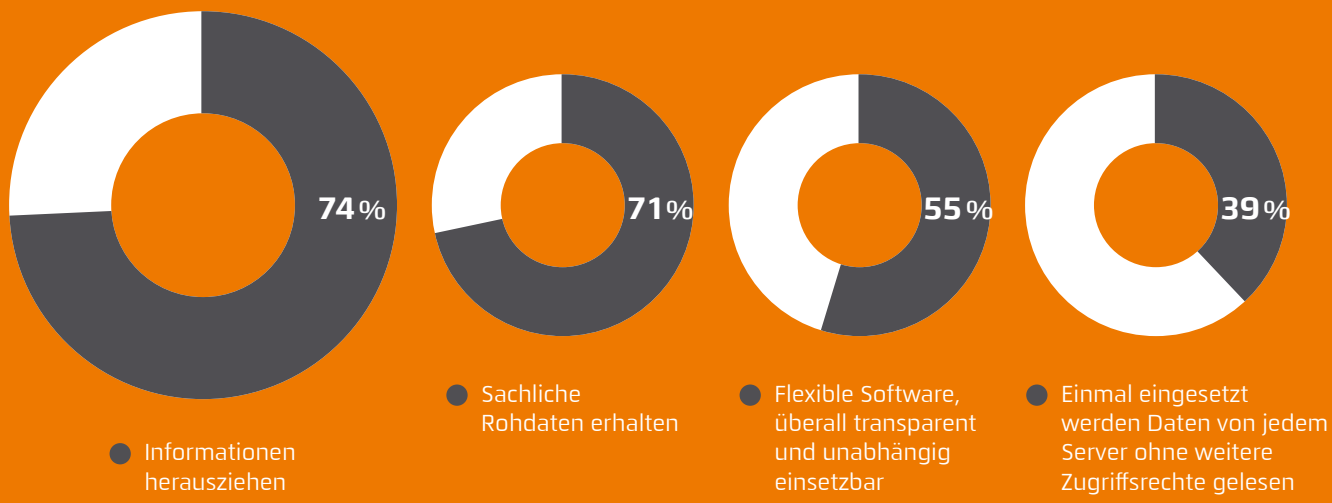
Unternehmen verwenden DPI aus verschiedenen Gründen. Für 42% der Befragten ist der wichtigste Grund, die Sichtbarkeit von Netzwerkwerkdaten sowie die Aussagekraft der Analysen zu erhöhen.

Weitere 28% geben an, die Einhaltung von IPS/IDS-Regeln zu verfolgen. Allein 21% haben das Ziel, die Untersuchungszeiten zu verkürzen und ganze 7% möchten den Umfang forensischer Daten einschränken.



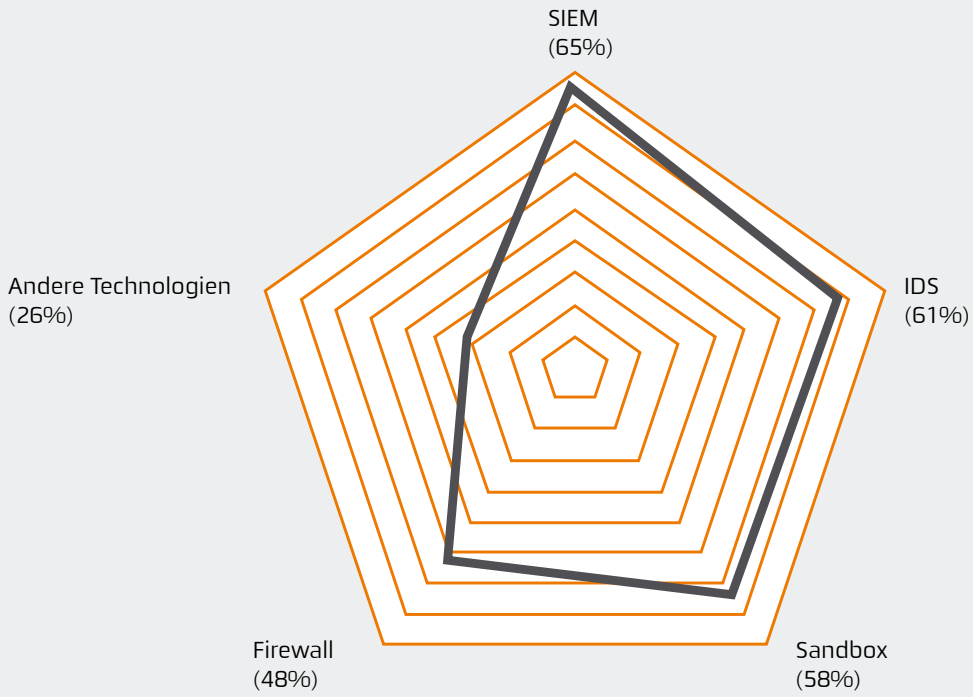
WAS SEHEN SIE ALS DEN HAUPTSÄCHLICHEN VORTEIL DER DPI SENSOREN?

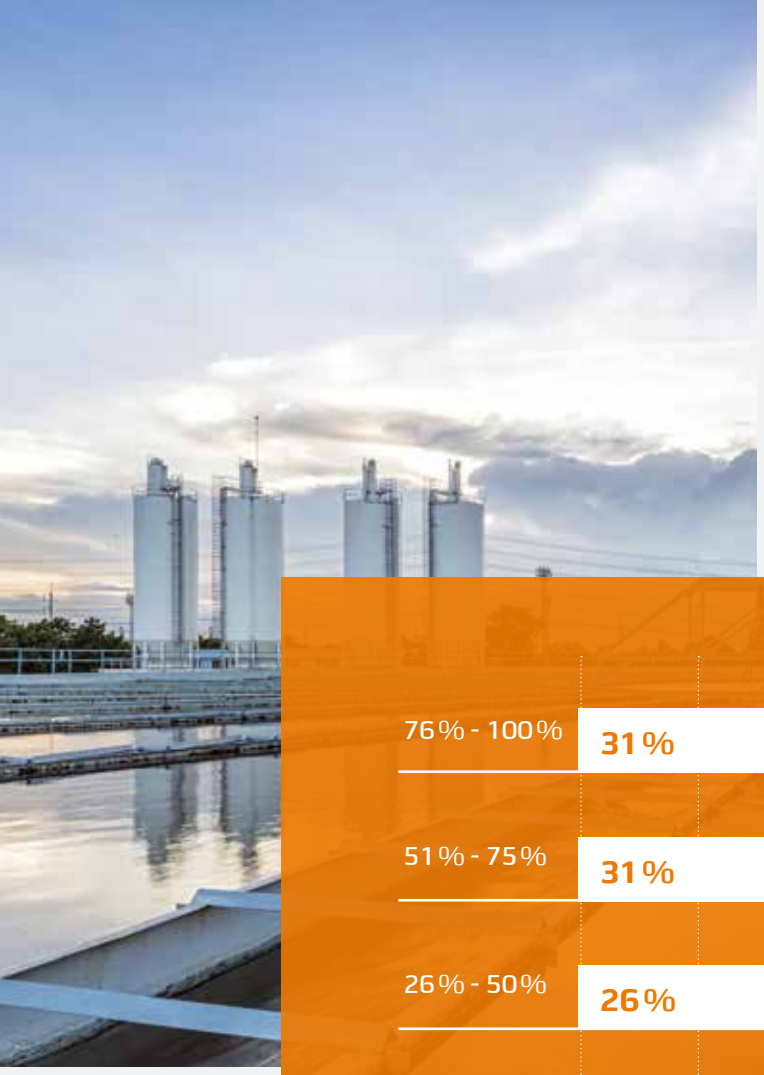
Bei der Frage nach den Vorteilen hoben 74% der Umfrageteilnehmer die Möglichkeit hervor, Informationen aus allen möglichen Assets (Web Mail, VoIP, Applikations-Server) herauszuziehen. Dicht gefolgt mit 71% der Befragten, denen es um die Vorteile beim Erhalt sachlicher Rohdaten (Telemetriedaten) geht.



MIT WELCHEM SYSTEM SOLLTEN DPI SENSOREN INTEGRIERT WERDEN?

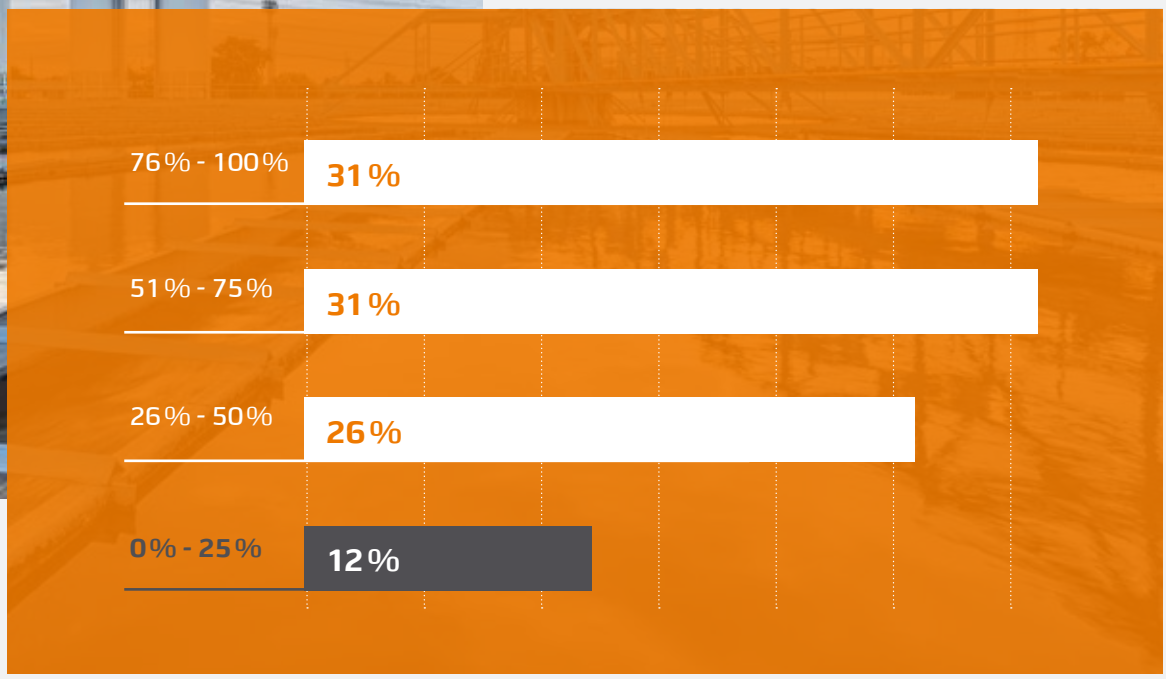
DPI Sensoren liefern Informationen zu einer Vielzahl weiterer Sicherheitstechnologien. Allein 65% der Befragten äußerten den Wunsch, dass DPI Sensoren in SIEM Systemen integriert sein sollten. Weitere 61% nennen die Integration in IDS, gefolgt von Arbeiten in der Sandbox mit 58%, eine Integration in der Firewall mit 48% und weitere andere Technologien mit 26%.





WELCHER PROZENTSATZ DIESER SENSOREN WÄRE VIRTUELL?

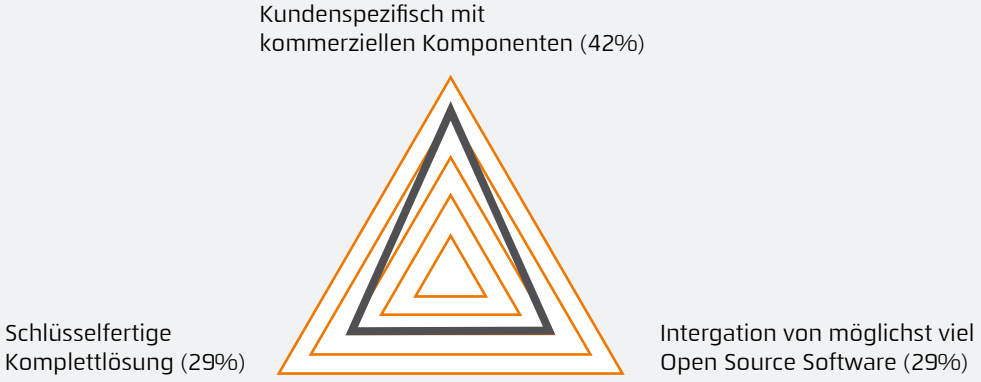
Eine Mehrheit von 62% der Befragten berichtet, dass sie über die Hälfte der DPI Sensoren auf virtuelle Instanzen verteilt sehen.

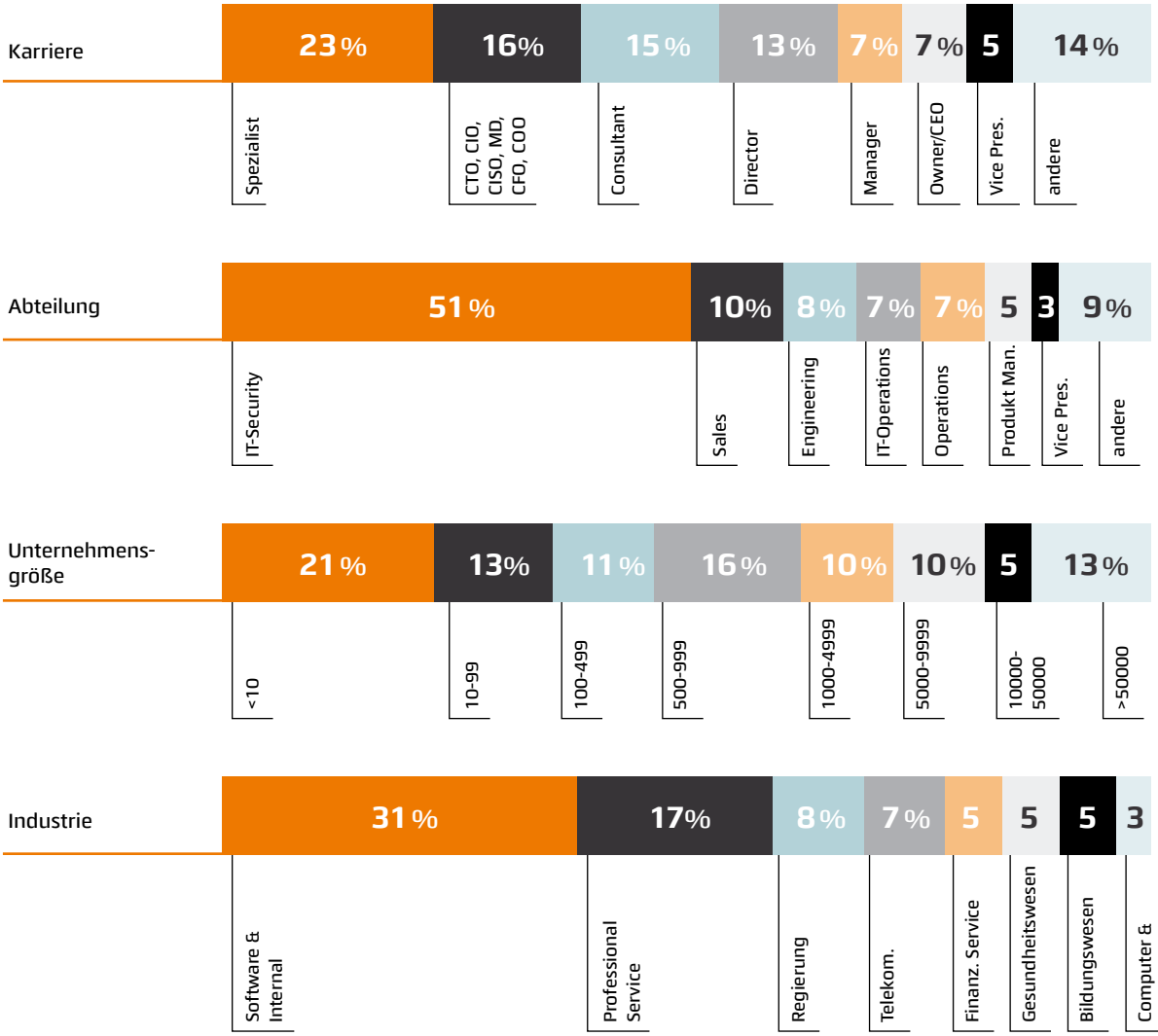


WELCHE DER FOLGENDEN LÖSUNGEN HILFT IHNEN BEI DER KOSTENMINDERUNG (TCO)?

Zur Frage nach der Kostenminderung bei Lösungen für die Netzwerkanalyse bevorzugen 42% der IT-Sicherheitsfachleute kundenspezifische Konzepte auf Basis kommerzieller Komponenten.

Dem gegenüber sind es bei der Integration von Open Source Software oder einer schlüsselfertigen Komplettlösung jeweils 29%.





METHODOLOGIE UND DEMOGRAFIE

Dieser Bericht basiert auf den Ergebnissen einer umfassenden Online-Befragung von Cybersecurity-Spezialisten. Er gewährt tiefe Einblicke in die Angriffe und die Sicherheit mit den vorhandenen Lösungen zur Abwehr. Die Betrachtung enthält den Bereich Deep Packet Inspection.

Wenn Sie Unterstützung bei der Verwendung von Fachbegriffen benötigen, können Sie auf unserer Webseite unter **https://videc.de/service/glossar** entsprechende Informationen abrufen.

* Original erschienen von Cybersecurity Insiders Holger Schulze, CEO and Founder sponsored by ENEA Qosmos Division

IRMA®

Erfahrung, Sicherheit, Vertrauen

25 Jahre Expertise im Bereich Automatisierung mit jahrzehntelangem Erfahrungswissen in Beratung und Umsetzung von Security Projekten von der Netzwerk- bzw. Anwendungssicherheit bis zum Security Management – darauf können Sie zählen.

Ob für kritische Infrastrukturen, produzierende Industrieunternehmen der verschiedensten Branchen oder Maschinen- und Anlagenbauer – das IRMA® System ist skalierbar und in das ISMS, SIEM sowie in die Bedienung und das Servicekonzept integrierbar.

Unser Konzept – Ihr Vorteil

- Einfach verständliche Produkte, die komplexe Problematiken lösen
- Tiefes Know-how in der Automatisierung und IT/OT Security sowie KRITIS Unternehmen
- Breites Partnernetzwerk sowie auch direkte Betreuung durch uns
- Schneller Einstieg durch Begleitung in der Einführungsphase und angepasste Schulungskonzepte
- Sicherer Betrieb durch technische Unterstützung, Updatekonzepte und gestaffelte Supportpakete

Sie wollen weitere Informationen zu OT Security – gerne.

Mit Videos,
Online Seminaren,
Infopapers,
Erfahrungsberichten

SecurITy made in Germany

Besuchen Sie unsere Webseite unter www.videc.de/irma-marktbetrachtung/ oder rufen Sie uns an.

VIDEC Data Engineering GmbH
Contrescarpe 1 · DE-28203 Bremen · Phone +49(0)421 – 33 950-0 · info@videc.de · www.videc.de
Niederlassungen und internationale Vertretungen entnehmen Sie bitte unserer Webseite.

VIDEC.

design: www.blaukontor.de
01/2022