Kundenjournal
Consist Software Solutions GmbH
September 2018

CONSISTNEWS

Fokus IT Security

Die vor Ihnen liegende Ausgabe der CONSISTNEWS gibt einen Einblick in unser Unternehmen und unsere Projekte. Den Schwerpunkt bilden zwei bemerkenswerte Best Practices zur IT Security, ergänzt um Nachrichten aus der Consist-Welt und kuriose Streiflichter aus der IT.
Wir wünschen Ihnen viel Spaß beim Lesen.

Insider Threat

Fehler vermeiden – Datenmissbrauch verhindern: User Access Management mit ObserveIT.

SIEM-Lösung

Implementierung eines sicheren, in Echtzeit operierenden Meldesystems mit Splunk.

Wenn viele Hände auf KRITISche Daten zugreifen müssen

Im hektischen Klinikalltag müssen viele Arbeitsabläufe auf Basis sensibler Patientendaten ineinandergreifen. Interne wie externe Dienstleistungen sind darin involviert und damit verbunden der Zugriff auf die entsprechenden IT-Daten. Gestiegene Datenschutz-Auflagen verlangen nun den Nachweis darüber, dass der Schutz von Patienten- und Mitarbeiterdaten in sämtlichen Leistungsprozessen gewährleistet ist.
Ein großes Klinikum hatte daher frühzeitig ein System implementiert, das den Schutz der Krankendaten gegenüber externen Dienstleistern sicherstellen sollte. Allerdings kam es in der Folge zu Performance-Problemen, da die integrierte Software zu viele Ressourcen verbrauchte.

Der Gesundheitsversorger wandte sich daraufhin mit dieser

Herausforderung an Consist:

- Mehrere externe IT-Dienstleister besitzen Zugriff auf Datenbank-Server.
- Bisherige Überwachungssoftware reduzierte die Performance der Server und erschwerte die Wartungsunterstützung durch externe Dienstleister.
- Sicherung des gesamten IT-Systems, auch nach neuer EU-DS-GVO, unter Einhaltung verschärfter KRITIS-Auflagen, bei gleichzeitigem Bestand der Zugriffsrechte.
- Überwachung in Echtzeit mit sofortiger Benachrichtigungsmöglichkeit.
- Integration einer Datenschutzlösung, die zugleich ressourcenschonend und nachweisfähig ist.

Gemeinsam mit der Fachabteilung fand man bei Consist eine Lösung, die ressourcenschonend (zugleich

„Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen."
(Auszug aus Definition des BBK)

KRITIS-Sektoren*:

- Energie
- Informationstechnik & Telekommunikation
- Gesundheit
- Wasser
- Ernährung
- Transport und Verkehr
- Finanz- & Versicherungswesen
- Staat & Verwaltung
- Medien & Kultur

Ab wann ein Unternehmen als Betreiber kritischer Infrastrukturen im Sinne des Gesetzes gilt, wird durch die Kritisverordnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geregelt. Betreiber kritischer Infrastrukturen, die darunterfallen, müssen IT-Sicherheitsmaßnahmen nach dem „Stand der Technik" vorsehen und dem BSI erhebliche IT-Störungen melden.

*Quelle: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

eine Vorgabe der EU-DSGVO) die Entwendung kritischer Daten verhindert. Darin einbezogen wurden sämtliche Anforderungen der neuen EU-Verordnung:

Die Lösung mit Consist

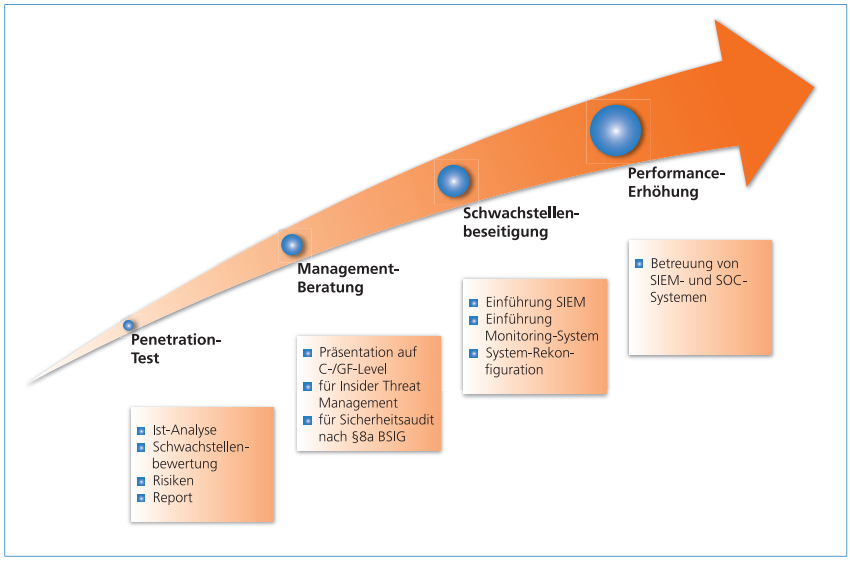
- Hoch performante Datenbank-Sicherheitslösung auf Basis von ObserveIT, die sich in die restriktiven User-Rechte-Einschränkungen des Krankenhauses einfach integrieren lässt.
- Integration einer Forensik- und Risikomanagement-Lösung, die ausschließlich reine User-Handlungen protokolliert und keine unnötigen Metadaten. Dadurch entsteht weniger Speicherbedarf als bei vergleichbaren Lösungen.
- Aufsetzen auf vorhandenen Windows-Betriebssystemen (Server und Desktop) und Citrix-Systemen.

Im Klinikalltag hat sich diese Lösung bewährt und ist auch für Unternehmen, die nicht unter die verschärften KRITIS-Bestimmungen fallen, eine effiziente Antwort auf die Datenschutz-Forderungen der EU-DSGVO. ■

Das Mehr an IT-Sicherheit erreichen

Big Data und der Trend zur Vernetzung von immer mehr Informationen sowie ständig neue Sicherheitsbedrohungen erfordern ein hohes Sicherheitsmaß in der IT-Infrastruktur. Personenbezogene Daten müssen aktuell im Sinne der EU-Datenschutzgrundverordnung verarbeitet und gespeichert werden. Informationen innerhalb und auch außerhalb des Unternehmens werden immer häufiger digital ausgetauscht. Für Angreifer aus dem Netz bieten sich also jede Menge Sicherheitslücken, um in teils sensible Dokumente Einblick zu erhalten.
Mit dem ganzheitlichen IT-Security-Konzept von Consist erfüllen Sie gesetzliche Sicherheitsauflagen nachweislich und verbessern die Performance Ihrer IT nachhaltig.

Wichtige Bausteine, die modular eingesetzt werden können, sind im Rahmen einer Sicherheitsstrategie (s. Grafik):



Nach der Aufnahme des Ist-Zustandes werden auf Wunsch in Workshops integrierte Lösungsfindungen erarbeitet, die entsprechenden Systeme eingeführt und von den Managed Security Services betreut.

observe it

Mit ObserveIT steht Ihnen eine zentrale Lösung zu Data Loss Prevention (DLP) und User Access Management (UAM) für sämtliche gängigen Betriebssysteme und Plattformen zur Verfügung.
ObserveIT ist die führende und derzeit einzige datenschutzkonforme Insider-Threat-Management-Lösung mit mehr als 1.800 Kunden verschiedenster Branchen in 87 Ländern.
Der Gartner-Marktreport 2018 attestiert ObserveIT die bestmögliche Einsicht in Benutzeraktivitäten einer Organisation. 2017 wurde ObserveIT als beste Insider-Threat-Lösung mit dem Cyber Security Award ausgezeichnet. ■

Splunk – BAITman für den Bankbetrieb

Im Hintergrund des Bankgeschäftes laufen komplexe IT-Systeme und -Prozesse, die beispielsweise Kennzahlen für Risikomanagement und Controlling aggregieren, aufbereiten und melden oder spezielle Algorithmen im Trading einsetzen. Die Folge ist ein Datenhype, für den zu jeder Tages- und Nachtzeit Integrität, Verfügbarkeit und Sicherheit gewährleistet sein muss.

Diese Masse an Datenströmen bringt die Gefahr mit sich, an vielen Stellen fehlgeleitet, angezapft oder falsch bedient werden zu können. Banken stehen daher vor der Aufgabe, jeden einzelnen Systemzugriff durch ein gezieltes Monitoring überwachen zu müssen - seit Ende letzten Jahres ein konkreter Bestandteil der Bankaufsichtlichen Anforderungen an die IT (BAIT).

Innerhalb der Finanzbranche konnte Consist nun in einem Kundenprojekt das dafür nötige zentrale Sicherheitsinformations- und Ereignismanagement (SIEM) installieren, das sicher ist und in Echtzeit operieren kann.

Die Herausforderung

- Besonderheit: Mehr als 40 heterogene Systeme mit sehr hohem Schutzbedarf einschließlich SAP vorhanden, die eingebunden und überwacht werden müssen
- Etablierung eines zentralen aktuellen Standardsystems, jederzeit erweiterbar um neue Anwendungen
- Implementierung eines sicheren, in Echtzeit operierenden Meldesystems

Die Umsetzung

- Proof of Concept
- Projektteam mit internen Spezialisten des Kunden (Projektleitung und Fachanwendungsbetreuer) und externen Spezialisten von Consist (zertifizierte Splunk- und Security-Berater)
- Beratung und Unterstützung hinsichtlich der Architektur, Systemauslegung und des Betriebs
- Aufsetzen und Inbetriebnahme eines Standardsystems inkl. Einbettung in die kundentypischen Entwicklungs-, Test-, und Produktivsetzungsprozesse (z. B. durch Staging)

Das Ergebnis

- Risikominimierung durch Einbindung auch hoch-privilegierter Nutzer ins Monitoring
- Aufdeckung von Inside Threats
- Revisionsfestes, nicht manipulierbares Sicherheitssystem, das in Echtzeit agiert
- Erfüllung der BSI-, EZB- und BaFin-Sicherheitsanforderungen

Alle Anwenderprozesse privilegierter Nutzer sind dadurch revisionsfest und nach den neuesten Sicherheitsbedingungen von EZB und BaFin in den Bankalltag integriert. Auf Wunsch des Kunden erfolgte der fließende Übergang in die Anwendungsbetreuung der Managed Services von Consist. ■

splunk>

Die heutige IT bewegt sich im Spannungsfeld immer größerer heterogener Datenmengen und häufig geänderter Anforderungen an die IT-Umgebung. Gleichzeitig steigen die Ansprüche an Datenauswertungen, möglichst in Echtzeit sowohl den internen IT-Service als auch sämtliche Business-Prozesse zu optimieren. Im nächsten Schritt folgt die vorausschauende Steuerung, indem zukünftige IT-, Sicherheits- und Geschäftsergebnisse vorhergesagt werden.

Einfach zu bedienende Dashboards von Splunk

An dieser Stelle kommen IT Operations Analytics mit Splunk ins Spiel. ITOA-Lösungen sind in der Lage, Datenströme unterschiedlichster Quellen zu sammeln und zu analysieren. Nur wenige Lösungen können dies jedoch so umfassend wie Splunk. Als universelle Plattform automatisiert Splunk das Sammeln und Indizieren von Maschinendaten sowie Analysieren und Visualisieren der empfangenen Informationen unabhängig von deren Speicherort. Splunk ermöglicht so infrastrukturübergreifend Machine-Learning-Analysen und löst automatisiert Benachrichtigungen aus, die für die Prozesse eines Unternehmens wichtig sind.

Splunk Inc. ist der führende Anbieter von Operational Intelligence-Software, mit der Echtzeit-Computerdaten sowie Terabytes von historischen Daten vor Ort oder in der Cloud überwacht, analysiert und in Berichten dargestellt werden. Mehr als 7.900 Unternehmen, Universitäten, behördliche Einrichtungen und Service Provider in 110 Ländern nutzen Splunk, um Service-Levels zu verbessern, IT-Betriebskosten zu reduzieren, Sicherheitsrisiken zu verringern und die Transparenz betrieblicher Prozesse zu erhöhen. Seit mehr als fünf Jahren setzt Consist Splunk in Big-Data-Projekten ein. ■

Vor kurzem konnten wir die erfolgreiche fünfjährige Partnerschaft zwischen Consist und Splunk feiern. Milestones finden Sie in unserer Broschüre auf www.consist.de/splunk

Consist gewinnt den „Boss of the Soc Award". Bei der .conf2017 setzte sich das Consist-Team gegenüber 100 teilnehmenden Expertenteams aus aller Welt durch. Am 1.10.2018 stellen sich unsere Consultants auf der internationalen Konferenz in Orlando erneut dieser Herausforderung. Wir drücken die Daumen!

Consist, wer wir sind

Seit 35 Jahren erfolgreich am Puls der Zeit

Für ein etabliertes Unternehmen wie Consist ist es eine große Herausforderung, die sich ständig verändernden Märkte und Kundenbedürfnisse wahrzunehmen und sich immer wieder neu darauf einzustellen.
Dies gilt umso mehr in der IT, deren kurze Innovationszyklen eine laufende Justierung des eigenen Leistungsangebots erfordern.
Consist ist stolz darauf, sich bereits seit 35 Jahren erfolgreich im Markt zu positionieren – und arbeitet mit Hochdruck daran, diesen Erfolg mit weiteren marktnahen Veränderungen langfristig fortzuschreiben.
Anfang des Jahres wurde die Geschäftsführung verstärkt um Jörg Hansen, der nun gemeinsam mit Daniel Ries und Martin Lochte-Holtgreven die wichtigen Zukunftsthemen rund um Security und Digitalisierung weiter vorantreiben wird.
Mehr als 200 Mitarbeiter kümmern sich tagtäglich bei Consist darum, dass Ihre Projekte, die wir mit Ihnen als unseren Kunden gemeinsam entwickeln oder zukünftig entwickeln wollen, reibungslos laufen. ■

Das Consist-Team 2018 auf dem jährlichen Mitarbeiterevent

Was Sie noch interessieren könnte

Spende an das Kinderhaus „Blauer Elefant“

Mit der jährlichen Unternehmensspende von 4.000 Euro zeigt Consist sein soziales Engagement, immer mit Bezug zur Region. Dabei wählen die Mitarbeiter aus, welche Organisation die Spende erhält. Diesmal fiel die Wahl auf den „Blauen Elefanten“. Die Einrichtung hat zum Ziel, Kindern und Jugendlichen in einem geschützten Raum die Möglichkeit zu geben, ihre Fähigkeiten und Stärken zu entwickeln. ■

Scheckübergabe an das Kinderhaus durch Martin Lochte-Holtgreven

Fachartikel und Studien

Wir veröffentlichen Fachartikel zu speziellen Themen in diversen Magazinen. Artikel zum Thema Insider Threats finden Sie zum Download auf unserer Webseite unter www.consist.de/observeit

<kes> - Microsoft-Sicherheitsstudie 2018: Consist beteiligt sich mit Sponsoring und Fragenstellung an der diesjährigen Sicherheitsstudie von Microsoft und <kes>, der Fachzeitschrift für Informations-Sicherheit.
Alle zwei Jahre fragt die <kes> nach Erfahrungen aus der Praxis und möchte mit dem Fragebogen zur Studie gleichzeitig eine Checkliste für die IT-Sicherheit liefern. Ziel ist es, verlässliche und neutrale Zahlen zur Informationssicherheit in Unternehmen und Behörden zu erhalten. Teil 2 der Ergebnisse zur Studie wird am 01.10.2018 veröffentlicht. Sprechen Sie uns bei Interesse gerne an. ■

„Versorgungsunternehmen im Spannungsfeld Datensicherheit“ im ew-Magazin Stadtwerke

„Outsourcing von IT-Dienstleistungen: Chance oder Risiko?“ im <kes> Special Referenzprojekte

Wo Sie uns finden – Consist auf Veranstaltungen

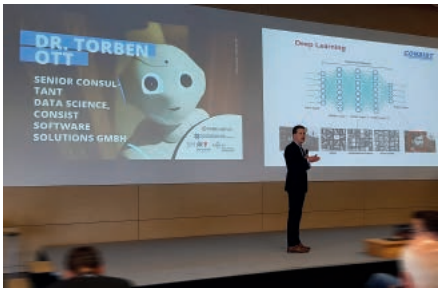
Consist ist auf vielen Veranstaltungen – regional, bundesweit und international – präsent. Bei der Auswahl liegen die Schwerpunkte auf unseren Fokusthemen IT Security und Digitale Transformation. Unsere aktuellen Projekte spiegeln den Bedarf unserer Kunden darin wider. Die folgenden Impressionen zeigen einige Beispiele erfolgreicher Veranstaltungen und eine Vorausschau auf noch anstehende in diesem Jahr.

OIT User Conference im Rahmen der secIT am 6.3.2018: mit Use Cases von Anwendern und Real Life Experiences zum Thema Threat Management

Heise Security Tour im April und Mai 2018: Beteiligung mit einem Ausstellerstand zum Thema IT Security

ITF.SH Innovations- und Technologieforum Schleswig-Holstein | SH Schleswig-Holstein Landesregierung

3. Innovations- und Technologieforum Schleswig-Holstein am 2. Mai 2018: Impulsvortrag Digitalisierung von Martin Lochte-Holtgreven



Künstliche Intelligenz – Perspektiven für Schleswig-Holstein am 31. Mai 2018: Vortrag zum Thema „Bilderkennung – Deep Learning im Praxiseinsatz"

Digitale Woche Kiel vom 8.-15.9.2018: Beteiligung mit Vorträgen zu Machine Learning und Digitalisierung

Moderation auf der Rethink! IT Security vom 26.-27.4.2018 sowie der Rethink! IT DACH vom 16.-18.9.2018

Norddeutscher Versorgertag am 7. Juni 2018 und 7. VKU-IT-Kongress am 28.-29.11.2018: Fachvortrag und Ausstellerstand zum Thema IT-Security

DIALOGUM CONNECTING BUSINESS
21. November 2018
16. LOGISTIK- & SCM-GIPFEL

Moderation eines Round Tables zum Thema „SCM Babylon?! Ist die Supply Chain wirklich durchgängig digitalisierbar?

Hackerangriff während PoC aufgedeckt

Ein Energieversorger plante, seinen Netzwerkverkehr und die Netzwerk-Infrastrukturkomponenten zu überwachen, und suchte dafür die passende Lösung. In einem Proof of Concept (PoC) sollte Consist aufzeigen, dass Splunk für diesen Zweck das Mittel der Wahl ist.

So installierte Consist Splunk mit einer Cisco-App und band die Netzwerkkomponenten an. Grafisch aufbereitet wurden während des PoCs die Verbindungsversuche mit dem Firmennetzwerk auf einer Weltkarte im Dashboard dargestellt. IP-Adressen können mit Splunk nämlich mühelos mit Geo-Locations angereichert werden.

Aus der Darstellung ging hervor, dass die gängigen Suchmaschinen, andere bekannte Institutionen und eigene Niederlassungen auf das Netzwerk zugriffen. Mit großen Augen entdeckten die Teilnehmer des PoCs jedoch auch ganz unerklärliche Verbindungen. Es handelte sich um dubiose Zugriffe aus der Ukraine, wie sich durch eine weitere Internetrecherche herausstellte, die direkt im Präsentationstermin vorgenommen wurde. Die entsprechenden IP-Adressen konnte der Energieversorger dann schnell sperren und dadurch wieder die nötige IT-Sicherheit herstellen.

Der Aha-Effekt war groß – und die Entscheidung für Splunk gefallen. Bessere Argumente, als einen Sicherheitsangriff von außen direkt während des PoCs festzustellen, kann es wohl gar nicht für den sinnvollen Einsatz einer Lösung geben. ■

Haben Sie Fragen? Rufen Sie uns gern an.

Consist Software Solutions GmbH
Christianspries 4
24159 Kiel
www.consist.de

Ihr Ansprechpartner:
Stefan Balzeit
0431-39 93-544
balzeit@consist.de

Impressum

Herausgeber
Consist Software Solutions GmbH
Christianspries 4, 24159 Kiel
04 31 / 39 93 - 525
news@consist.de
www.consist.de

Geschäftsführung
Daniel Ries, Martin Lochte-Holtgreven, Jörg Hansen
Redaktion
Isabel Braun, Ute Jansen,
Petra Sauer-Wolfgramm

Bildnachweise
Consist: S. 3, 5, 6, 7, 8
Adobe Stock: S. 1, 2, 4, 8

Druck
Lithographische Werkstätten Kiel