ProSoft

NETZWERK

LOG MANAGEMENT

IT-SICHERHEIT NACH BRANCHENSPEZIFISCHEN SICHERHEITSSTANDARDS (KRITIS / B3S) DER ENERGIE- UND WASSERVERSORGER

INNOVATIONSPREIS-IT
BEST OF 2018
initiative mittelstand
IT-SECURITY

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

Zur Gewährleistung der Nachvollziehbarkeit von sicherheitsrelevanten Aktionen bei Energie- und Wasserversorgern gemäß ISO27001/19 und KRITIS Branchenstandard (B3S) sowie aufgrund gesetzlicher Anforderungen an den Datenschutz muss Protokollierung eingeführt werden, welche die Nachvollziehbarkeit z. B. von Störungen, Warnungen, Informationssicherheitsvorfällen, Ausnahmen sowie Datenzugriffen von Benutzern und Administratoren entsprechend der gesetzlichen Vorgaben gewährleisten sollte. Eine ordentliche Protokollierung von Datenzugriffen und Veränderungen von Benutzerrechten ist heute nicht nur gesetzlich vorgeschrieben, sondern hilft Ihnen auch dabei, echtzeitnah auf Datenmissbrauch oder -verlust zu reagieren. Log Management mit auditsicheren Berichts- und Alarmierungspaketen wird damit zur Notwendigkeit für den sicheren Betrieb Ihrer Office- und Anlagen-IT.

Log Management ist keine Kür — sondern Pflicht

Zahlreiche Gesetzgebungen nehmen den Datenschutz und die Datensicherheit im Unternehmen immer stärker in den Fokus und erwarten entsprechend etablierte Maßnahmen.

IT-Sicherheitsgesetz (ITSiG)

Nach §8a des IT-Sicherheitsgesetzes sind Betreiber Kritischer Infrastrukturen seit dem 18. Juli 2017 verpflichtet, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme [...] zu treffen."

BSI-KritisV 1.0

Das IT-Sicherheitsgesetz ändert und ergänzt neben dem BSI-Gesetz auch das Telemediengesetz, das Telekommunikationsgesetz, das Atomgesetz, das Energiewirtschaftsgesetz und weitere Gesetze. Dabei entwickelt und veröffentlicht das BSI regelmäßig mit Branchenverbänden neue branchenspezifische Sicherheitsstandards (B3S).

Branchenspezifischer Sicherheitsstandard für die Verteilung von Fernwärme (B3S VvFw)

Der B3S VvFw legt fest, dass die nachhaltige und angemessene Behandlung aller relevanten Themenfelder zur Umsetzung der gesetzlichen Anforderungen nach § 8a Abs. 1 BSIG, z.B. durch den Betrieb eines Informationssicherheitsmanagementsystems (ISMS) in Anlehnung an ISO/IEC 27001:2013 sichergestellt wird. Der B3S VvFw findet Anwendung auf informationstechnische Systeme, Komponenten oder Prozesse der kritischen Infrastruktur Fernwärmenetz, d.h. auf IT-Systeme der Prozessdatenverarbeitung zur Messung, Steuerung und Regelung, die für die Funktionsfähigkeit der Verteilung von Fernwärme (VvFw) maßgeblich sind.

Quelle B3S: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Branchenspezifischer Sicherheitsstandard für Anlagen oder Systeme zur Steuerung / Bündelung elektrischer Leistung (B3S Aggregatoren)

Der Geltungsbereich dieses B3S und das geforderte ISMS umfasst alle Bestandteile, die für den Betrieb einer Anlage oder eines Systems zur Steuerung / Bündelung elektrischer Leistung erforderlich und für deren Funktionsweise essentiell sind:

- sämtliche zur Messung, Steuerung und Regelung und deren Planung erforderlichen zentralen IT-Infrastrukturen (z. B. SCADA-Applikationen, Regelungs- / Steuerungskomponenten, Energiedatenmanagement- und Überwachungssysteme, zentrale Datenbanken mit direkter Anbindung an das Steuer- / Leitsystem)

- sämtliche zum Betrieb der oben genannten IT-Infrastrukturen sowie zur Kommunikation mit den Erzeugungs- oder Verbrauchsanlagen und Netzbetreibern notwendigen zentralen Netzwerke, Firewalls, Gateways, Router etc.

- Betriebsstandorte des Aggregators wie z. B. Leitwarten, Rechenzentren, Technik-räume, etc.

Branchenspezifischer Standard „IT-Sicherheit Wasser/Abwasser" (B3S)

DVGW und DWA haben den B3S entwickelt, der sowohl den von der BSI-KritisV betroffenen Unternehmen wie auch kleinen und mittleren Wasserver- und Abwasserentsorgungsunternehmen ein Instrument an die Hand gibt, um ein Schutzniveau zu implementieren, das dem Stand der Technik entspricht. Das BSI hat die Eignung des IT-Sicherheitsstandards für den Sektor Wasser gemäß § 8a (2) BSI-Gesetz festgestellt, bestehend aus dem DVGW-Merkblatt W1060 und der Web-Applikation "IT-Sicherheitsleitfaden". Beides dient der branchenspezifischen Identifikation notwendiger Schutzmaßnahmen gegen Bedrohungen der informationstechnischen Systeme, Komponenten oder Prozesse der Anlagen.

Datenschutz-Grundverordnung (DSGVO)

Die Datenschutz-Grundverordnung hat es sich zum Ziel gesetzt, die Grundrechte und Grundfreiheiten natürlicher Personen und deren persönliche Daten zu schützen. Die DSGVO wurde am 27. April 2016 verabschiedet und ist seit dem 25. Mai 2018 in allen EU-Mitgliedstaaten anzuwenden.

Personenbezogene Daten gemäß DSGVO sind alle Informationen, die sich auf eine natürliche oder betroffene Person beziehen und direkt oder indirekt zur Identifizierung dieser Person verwendet werden können. Dabei kann es sich um einen Namen, ein Foto, eine E-Mail-Adresse, Bankverbindungen, Beiträge in sozialen Medien, medizinische Informationen oder auch eine MAC-Adresse eines Computers handeln. Bei der Erhebung personenbezogener Daten müssen diese anonymisiert oder pseudonymisiert werden. Die Artikel 24, 25 und 28 thematisieren die IT-Sicherheit und eine klare Anforderung an ein Log Management.

Artikel 24

Das Unternehmen verpflichtet sich, dass sein Rechenzentrum geeignete technische und organisatorische Maßnahmen getroffen hat, um sicherzustellen, dass die Verarbeitung personenbezogener Daten in Übereinstimmung mit der DSGVO erfolgt.

Artikel 25

Die technischen und organisatorischen Maßnahmen stellen sicher, dass personenbezogene Daten nicht einer unbegrenzten Zahl natürlicher Personen zugänglich gemacht werden. Ein solcher technischer Schutz kann nur von einem Log Management gesetzt und bei Prüfung bewiesen werden.

Artikel 28

Das Unternehmen kann nachweisen, dass sein Rechenzentrum Überlegungen bezüglich personenbezogener Daten angestellt hat, welche Daten personenkritisch sind, welche Applikationen darauf zugreifen können und wie die Daten vom Unternehmen geschützt werden. Dies muss für eine mögliche Prüfung durch einen Auditor dokumentiert sein.

Quelle BDSG: Bundesministerium der Justiz und für Verbraucherschutz

Bundesdatenschutzgesetz (BDSG)

Das BDSG stellt mit §76 klare Anforderungen an eine Protokollierung von Daten in Unternehmen:

„(1) In automatisierten Verarbeitungssystemen haben Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren: Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung.

(2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen.

(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten, die Bundesbeauftragte oder den Bundesbeauftragten und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.“

Geschäftsgeheimnisgesetz (GeschGehG)

Das GeschGehG befasst sich mit dem Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.

Nehmen wir an, ein (ehemaliger) Mitarbeiter stiehlt vertrauliche Daten und gibt diese an Dritte weiter. Bisher war so ein Fall recht einfach, da Sie die gestohlenen Daten als „geheime Geschäftsdaten“ melden und den Mitarbeiter vor Gericht belangen konnten. Durch das Inkrafttreten des GeschGehG sind Unternehmen nun allerdings angehalten, den Zugriff auf ihre Geschäftsgeheimnisse durch entsprechende technische und organisatorische Maßnahmen zu schützen. Finden sich die geheimen Daten nicht dokumentiert in solchen Maßnahmen wieder und wird der Zugriff auf sie nicht kontrolliert und protokolliert, lässt sich der Mitarbeiter für die Entwendung und Offenlegung der Daten nicht vor Gericht belangen.

„Mit den fertigen Berichts- und Alarmierungspaketen von ProLog erfüllen wir die vielfältigen regulatorischen Anforderungen an die Protokollierung von Events in unserer Anlagen- und Office-IT. Durch die Auswertung der Berichte und Alarmierungen können wir schnell und zielgenau auf Unregelmäßigkeiten reagieren. ProLog hilft dabei sicherheitsrelevante Themen im Blick zu haben und bietet die Möglichkeit der zentralen forensischen Untersuchung im Fall der Fälle.“

— Christoph Rosport, IT-Service,
enwag energie- und wassergesellschaft mbh

ProLog: Auditsicheres Log Management in 4 Schritten

Auch wenn am Ende kein Weg daran vorbeiführt, haben Sie vermutlich weder die Zeit noch das Interesse, sich bis ins Detail mit dem Thema Log Management zu beschäftigen. Es ist uns daher ein Anliegen, Ihnen eine auditsichere Lösung an die Hand zu geben, bei der Ihnen der Großteil der Last abgenommen wird. Das Softwarepaket ProLog unseres Partners NETZWERK Software GmbH tut das in genau vier Schritten:

1

Dokumentation

Innerhalb von zwei Tagen erstellen wir mit Ihnen gemeinsam ein etwa 40-seitiges Dokument, das alle IT-sicherheitsrelevanten Notwendigkeiten und Definitionen festhält. Welche Daten sind personenbezogen und kritisch, und welche nicht? Welche Applikationen sollen in das Log Management eingebunden werden? Diese Dokumentation behalten Sie als Nachweis für zukünftige Audits, dass Sie sich Gedanken zu diesen Themen gemacht haben.

2

Umsetzung in der Software

Wir übertragen die festgelegten Anforderungen in die ProLog-Software und installieren diese in Ihrer IT als Blackbox. Innerhalb von ProLog sind technische und organisatorische Maßnahmen (TOMs) wie beispielsweise Pseudonymisierung, granulare Rollenkonzepte und N-Augen-Prinzip fest implementiert. Damit stellen wir sicher, dass kein IT-Administrator bewusst oder unbewusst gegen die Datenschutz-Grundverordnung verstößt.

3

Alarmierung und Berichte

Die von ProLog erstellten Berichtspakete entsprechen einem sich immer weiter entwickelten Standard für Ihre Branche. Sie erhalten täglich, wöchentlich oder monatlich auditsichere Berichte, die um einen individuellen Informationsbedarf ergänzt werden können. Alarmierungen helfen Ihnen außerdem dabei, den Zugriff auf geschäftskritische Daten zu überwachen, Benutzerrechte sauber zu pflegen oder Fehler im System zu finden.

4

Wartung

Wir pflegen die Software auch nach der Installation weiter für Sie. Damit wird sichergestellt, dass Ihre Alarmierungen und Berichte auch nach einem Wechsel von Systemkomponenten ordentlich funktionieren. Außerdem erhalten Sie automatische Updates, sollten sich gesetzliche oder andere Anforderungen geändert haben. Auch individuelle Anfragen von Auditoren werden beantwortet und in einem weiteren Schritt vorsorglich für alle Kunden in den Standard übernommen.

Die Experten für Log Management

ProSoft GmbH

Gemäß dem Slogan „Manage, Secure, Optimise IT“ steht ProSoft seit der Gründung im Jahr 1989 für effiziente IT-Security & IT-Management-Lösungen. Darüber hinaus arbeitet das Unternehmen mit Premium „Hidden Champions“ und deren Alleinstellungsmerkmalen, um alle Kundenanforderungen exakt zu bedienen und die Lücken der Standardanwendungen zu schließen.

ProSoft sorgt mit seinen Managed Services und Support für IT-Sicherheit in der Infrastruktur in Unternehmen – branchenübergreifend. 36 von 40 DAX-Unternehmen und über 5.000 Kunden in der DACH-Region nutzen die Lösungen von ProSoft. Darüber hinaus unterstützt das Unternehmen als Value-Added-Distributor (VAD) Hersteller beim „Go-to-Market“ und der Markteinführung neuer Lösungen im deutschsprachigen Teil Europas. Im Fokus stehen dabei Mehrwerte für Reseller und institutionelle IT-Anwender. Hersteller profitieren von den firmeninternen Marketing- und Vertriebsstrategien und Services wie Webcasts, Events, Partnertrainings, Installations- und Produktsupport.

ProSoft GmbH
Bürgermeister-Graf-Ring 10
82538 Geretsried

Tel.: +49 8171 405-0
E-Mail: info@prosoft.de
www.prosoft.de

NETZWERK Software GmbH

Die NETZWERK Software GmbH ist der deutsche Anbieter und Entwickler der Log Management-Lösung ProLog. Protokollierung ist ein branchenübergreifendes Thema mit einer breiten Kundenbasis. Wir betreuen Kunden aus den Bereichen Mittelstand, Finanz- und Versicherungswesen, Energie- und Wasserversorgung, Gesundheit, Wohlfahrt und Kirche, öffentliche Einrichtungen (Kommunen, Länder, Bund), Kammern und Verbände, Automobilzulieferer und viele mehr.

Die NETZWERK betreibt Forschung im Bereich IT-Security, unter anderem mit Bundesbehörden, mit der Fraunhofer FKIE und der Hochschule Regensburg. Als Teil des Teletrust-Verbands, eine Vereinigung der deutschen IT-Security-Hersteller, ist die NETZWERK mit dem Gütesiegel *Security made in Germany* ausgezeichnet. Wir sind Mitglied der Allianz für Cybersicherheit des Bundesamtes für Sicherheit in der IT (BSI) und wurden 2018 für ProLog mit dem Innovationspreis-IT der Initiative Mittelstand gekürt.

NETZWERK Software GmbH
Adalperostraße 80
85737 Ismaning bei München

Tel.: +49 89 452 452-0
E-Mail: info@netzwerk.de
www.netzwerk.de