Datenschutzkonforme Protokollierung mittels iQSol LogApp

iQSol
Security made in Austria.

Datenschutzkonforme Protokollierung mittels iQSol LogApp

Whitepaper

Inhalt

1. EINLEITUNG

Datenschutz und Protokollierung: Was zunächst wie ein Widerspruch klingt, ist bei näherer Betrachtung keiner. Wer Datenschutz unter Einhaltung der rechtlichen Rahmenbedingungen erfüllt, ist aufgrund des Datenschutzgesetzes dazu aufgefordert, bestimmte Daten (Logs) zu speichern und bei Bedarf dem Gesetzgeber zu übergeben.

Datenschutzkonforme Protokollierung befasst sich im Wesentlichen mit zwei Punkten:

- Mit der Einrichtung einer zentralen Protokollierung aller datenschutzrechtlich relevanten Zugriffe auf personenbezogene, sensible, biometrische sowie genetische Daten.
- Mit der Umsetzung einer verordnungskonformen, zentralen Protokollierung unter Beachtung datenschutzrechtlicher Gesichtspunkte für die Protokollierung selbst (Manipulationssicherheit).

Ab wann ist nun aber ein Protokollierungsbedarf gegeben? Und ab wann erfüllt eine Protokollierung die Anforderung des Datenschutzes? Antwort geben Datenschutzexperten sowie das Datenschutzgesetz. Die technologische Seite wiederum kann aus dem BSI-Grundschutzhandbuch abgeleitet werden.

Das vorliegende Whitepaper soll diese verschiedenen Quellen und Anforderungen übersichtlich bündeln und auf dem Weg zu einer datenschutzkonformen Protokollierung unterstützen.

2. GRUNDSÄTZE DER PROTOKOLLIERUNG

Die Protokollierung von Daten und Bewegungen geht einher mit der Frage nach dem Schutz persönlicher Daten. Daher geben Bund und Länder einige Grundsätze für die Protokolldaten an die Hand, nach denen es sich zu richten gilt.

Dazu zählen unter anderem:

- **Transparenz:**
  Wer hat welche personenbezogenen Daten verarbeitet?

- **Zweckgebundenheit:**
  Personenbezogene Daten dürfen nur zweckgebunden, vollständig, aber datensparsam protokolliert werden. Der Zweck muss klar bezeichnet werden.

- **Unveränderbarkeit:**
  Personenbezogene Daten dürfen nicht nachträglich verändert werden.

- **Sicherstellung:**
  Kryptographische Verfahren zur Verschlüsselung und Signierung schützen Vertraulichkeit und Authentizität.

- **Funktionsfähigkeit:**
  Zur Sicherstellung funktionierender Technik müssen Tests durchgeführt werden. Änderungen am System müssen ebenfalls protokolliert werden.

- **Unterscheidbarkeit:**
  Protokolle müssen zwischen Aktivitäten von Maschine und Mensch sowie zwischen Administrator und Anwender unterscheiden.

- **Auswertung:**
  Protokolle dürfen nur nach den in der Dienstvereinbarung festgehaltenen Vorschriften ausgewertet werden.

3. ANFORDERUNGEN AN DIE PROTOKOLLIERUNG

Weitere Anforderungen an die Protokollierung sind zudem inhaltlicher sowie organisatorischer Natur. So wird vom Gesetzgeber gefordert, dass die Daten Auskunft über

- den sekundengenauen Zeitpunkt eines Ereignisses/einer Tätigkeit,
- seine/ihre Bezeichnung,
- die involvierte Person oder Server, Dienste, Services o.a. Systemkomponenten (Auslöser),
- den Zweck

geben.

Das Gesetz empfiehlt, sowohl Personen als auch Systemen einen Zugangsschlüssel zu geben, da dieser klarer identifizierbar ist. Darüber hinaus wird dem Grundsatz der Unveränderbarkeit ein Zusatz hinzugefügt: Werden Daten geändert, aus welchen Gründen auch immer, müssen diese vorher und nachher protokolliert und die Änderungen ganz genau benannt werden – mit Datum, Benutzerkennung, Tätigkeit und mehr. Auch, wenn Daten gelesen wurden, müssen diese benannt werden.

Wird nun zum Beispiel ein neuer Nutzer innerhalb des Systems angelegt (Zweck), löst dies zahlreiche Ereignisse an Systemen aus. Die Technik muss in der Lage sein, diese zu aggregieren und dann in einer Datenbank gesammelt und in einem für Analysewerkzeuge auslesbaren Format zu speichern.

Darüber hinaus werden folgende Punkte gefordert:

- **Datenübertragung:**
  Eine revisionssichere und datenschutzgerechte Protokollierung fordert die Übertragung über verschlüsselte Kanäle. Es wird eine Absicherung des Transportprotokolls mit TLS empfohlen.

- **Datenspeicherung:**
  Protokolldaten sollen auf eigenen Protokollservern mit strikten Zugangsregeln gespeichert werden. Dies gilt auch für Backups, das Datenlesen und die Datenverarbeitung.

- **Datenanalyse:**
  Eine Analyse von Protokolldaten mit Personenbezug darf nur nach dem Vier-Augen-Prinzip und unter Einbeziehung des Datenschutz- bzw. IT-Security-Beauftragten erfolgen. Werden die Daten zur Analyse weitergegeben, sollte eine Kontrollinstanz für Weitergabe, Verwendung und Löschung eingeführt werden.

- **Löschung:**
  Jedes Protokoll muss eine Aufbewahrungsdauer aufweisen. Ist diese abgelaufen, muss mit Hilfe des Datenschutzgesetzes darüber entschieden werden, ob es einen zwingenden Grund zur weiteren Aufbewahrung gibt oder nicht. Ist Letzteres der Fall, ist die Löschung Pflicht.

3.1. Erfüllung der Anforderungen einer Protokollierung zum Zwecke der Erfüllung der DSGVO

Unternehmen sehen sich folglich einigen Anforderungen gegenüber, die zu erfüllen sind. Im Folgenden soll nochmals tabellarisch aufgezeigt werden, welche diese sind – und wie sie mit Hilfe einer Appliance wie LogApp erfüllt werden können. LogApp ist eine IT-Sicherheitslösung, die mit einfachen Mitteln zahlreiche Log-Quellen sammeln und auswerten kann.

Anforderung	**Umsetzung mit iQSol LogApp**
Inhalt der Protokollierung – Zeitstempel	Sowohl Zeitstempel am Entstehungsort als auch Zeitstempel der Speicherung in der LogApp werden festgehalten. Eine Einbindung einer externen Zeitquelle ist mittels NTP möglich.
Inhalt der Protokollierung – Tätigkeit, Personen	Das Originalereignis wird unverändert abgespeichert. Zusätzlich können Detailwerte wie Benutzernamen oder Aktionscode mit Hilfe von Parsemaps in ein normalisiertes Format extrahiert werden.
Datenübertragung	Die Datenübertragung erfolgt von den Agenten mit TCP, Verschlüsselung erfolgt mit TLS. Netzwerkgeräte übertragen mit Syslog (UDP, TCP oder SSL). Der Einsatz von Proxys kann allenfalls die unverschlüsselte Strecke minimieren.
Vertraulichkeit - Zugriff	Zugriffsmöglichkeiten sind über ein rollenbasiertes Zugriffsmodell auf ein erforderliches Minimum reduzierbar. Löschen oder Verändern von Daten ist grundsätzlich nicht möglich. Alle Anmeldungen sowie alle Abfragen von Protokolldaten werden lückenlos protokolliert. Die Anmeldung mittels Multifaktorauthentifzierung ist möglich.
Vertraulichkeit - Mehr-Augen-Prinzip	Die Anwendung eines Vier-Augen-Prinzips ist auf alle Elemente (sowohl Konfigurationen als auch Analyse/Auswertungen) möglich.
Integrität und Vertraulichkeit – Langzeitarchiv	Die Daten im externen Langzeitarchiv werden signiert und können optional verschlüsselt abgelegt werden. Die Löschung der Daten des Langzeitarchives obliegt der Administration des Archivsystems. Daten des Langzeitarchives können durch die LogApp nicht gelöscht werden.
Datensparsamkeit	Die Daten werden lokal nach einer definierten Aufbewahrungsdauer in Tagen gelöscht. Die Festlegung selektiver Aufbewahrungsdauern pro Log-Quelle ist möglich. Anonymisierung ist sowohl persistent in der Datenbank als auch temporär am GUI (für Abfragen, rechtebezogen) möglich.
Verfügbarkeit	Eine garantierte Datenübernahme wird durch Agent-Buffer gewährleistet. Die vollständige Wiederherstellung einer LogApp ist durch Konfig-Backup/-Restore und Datenwiederherstellung aus dem Langzeitarchiv möglich.

3.2. Erfüllung der Anforderungen des BSI IT-Grundschutzkatalogs hinsichtlich einer sicheren Protokollierung

Der BSI IT-Grundschutzkatalog bringt zahlreiche Forderungen hinsichtlich einer sachgemäßen Protokollierung mit sich.

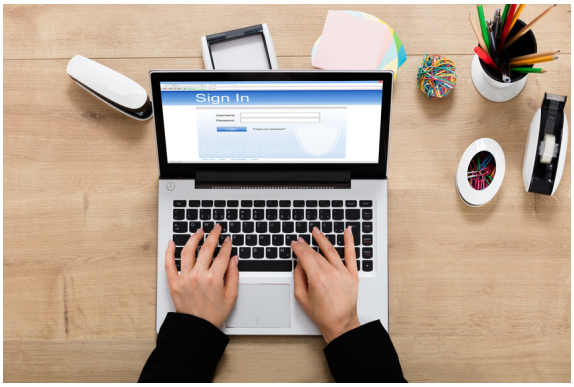
Die Anforderungen des BSI werden mittels iQSol LogApp durch folgende Funktionen abgedeckt:

BSI-Referenz	Anforderungen	Abdeckung
B 5.22	Zentrale Protokollierung	LogApp dient der zentralen Protokollierung heterogener Datenquellen (Server, Clients, Netzwerkgeräte usw.).
M 2.110	Protokollierung der Administrationsaktivitäten sowie der Benutzeraktivitäten	Protokolle können via Agenten (Windows, Linux) oder Syslog übernommen werden.
M 2.497, M 2.499	Platzierung im Netz (Trennung von Management und Protokollübertragung)	Die Verwendung von getrennten Interfaces für Management und Protokollübertragung ist möglich.
M 2.497, M 3.90, M 5.171	sichere Übertragung	Eine sichere Übertragung wird durch TLS auf allen Übertragungwegen gewährleistet.
M 2.497	Zugriff durch berechtigte Personen	rollenbasierte Benutzerverwaltung, LDAP-Integration, Vier-Augen-Prinzip
M 2.497	Relevante Systeme: • aktive Netzkomponenten • (z. B. Router, Switches) • Betriebssysteme • Applikationen und Dienste (z. B. Webserver, Mailserver, Fileserver) • Sicherheitskomponenten im Netz (z. B. Firewall, Proxy, IDS) • Sicherheitskomponenten auf Hosts (z. B. Sicherheitsgateways, Virus-Scanner) • physikalische Zutrittssysteme	Systeme können via Agenten (Windows, Linux, AIX) oder Syslog integriert werden. Die Agenten können sowohl System-Logs als auch Applikations-Logs übernehmen.
M 2.497	Daten sind laufend und möglichst in Echtzeit zuzuführen und regelmäßig auszuwerten.	Die Datenübernahme erfolgt nahezu in Echtzeit.
M 2.497, M 3.90, M 4.430	Frühwarnung/Alarmierung	Eine Analyse und Alarmierung ist regelbasiert möglich. Die Alarmierung erfolgt am GUI via E-Mail, Syslog oder über einen angebundenen iQSol Alert Messaging Server.

BSI-Referenz	Anforderungen	Abdeckung
M 2.497	Beweissicherung	Langzeitarchiv wird signiert und optional verschlüsselt.
M 2.500	Anmeldung unter administrativen Rechten sollte immer zu einem Eintrag im Protokoll führen	Übernahme von Protokollen beliebiger Vorgänge ist uneingeschränkt möglich.
M 2.500, M 4.227, M 5.172	Zeitsynchronisation	Die Einbindung einer NTP-Zeitquelle ist konfigurierbar.
M 2.500	Vertraulichkeit und Integrität der Protokolldaten	Die Vertraulichkeit und Integrität wird mittels einer rollenbasierte Benutzerverwaltung, LDAP-Integration, einem Mehr-Augen-Prinzip sowie der Signierung und Verschlüsselung des Langzeitarchivs sichergestellt.
M 3.90	Datum und Uhrzeit als zentrale Informationen. Je nach protokollerzeugendem System können diese unterschiedlich angeordnet sein.	Datum und Uhrzeit werden formatunabhängig übernommen und normalisiert abgelegt.
M 3.90	Unterstützung von Syslog	Syslog wird via UDP, TCP und SSL unterstützt.
M 3.90, M 4.431	Aggregation	Übertragung identer Protokollinformationen kann optional aggregiert werden.
M 3.90, M 4.431	Normalisierung	Alle Protokolldaten können mittels Parsemaps normalisiert werden.
M 3.90, M 4.431	Filterung	Die Selektierung der zu sammelnden Protokolldaten erfolgt mittels der Parsemaps, in welchenhier per White- und Blacklist-Mechanismen angewendet werden können.
M 3.90	Auswertung (aussagekräftige Darstellung der Ergebnisse in einer leistungsfähigen Benutzeroberfläche, Unterstützung bei der Erstellung von Berichten)	Grafische Auswertungsmöglichkeiten (Dashboards), Suche und Filterung sowie Enterprise Reporting sind verfügbar.
M 3.90	Archivierung (Mindestspeicherdauer, Löschpflicht)	Ein revisionssicheres Langzeitarchiv steht lokal oder auf einem externen Speicher zur Verfügung. Mindestspeicherdauer und Löschpflicht werden am externen Speicher verwaltet.
M 4.47, M 4.225	Protokollierung der Sicherheitsgateway-Aktivitäten	Sicherheitsgateways sind mittels Syslog integrierbar. Die Protokollmeldungen sind mittels Parsemaps normalisier- und filterbar.

BSI-Referenz	Anforderungen	Abdeckung
M 4.430	Berichterstellung	Berichte werden mittels eines Enterprise Reporting Server erstellt.
M 4.430	Grafische Darstellung	Alle gesammelten Protokolldaten lassen sich online darstellen, durchsuchen und filtern. Statistische Auswertungen stehen als frei konfigurierbare Widgets zur Verfügung.
M 4.430	Archivierung	Eine Archivierung aller gesammelten Protokolldaten erfolgt in einem signierten und optional verschlüsselten (externen) Langzeitarchiv.
M 4.431	Kategorisierung und Priorisierung	Die Kategorisierung von Protokolldaten wird mittels statischer Merkmale, die den Protokolldaten hinzugefügt werden können, unterstützt. Anhand von Auswertungsregeln können Ereignisse übersichtlich kategorisiert und priorisiert werden.
M 4.431	Korrelation	Es stehen zahlreiche Korrelations- und Gruppierungsmöglichkeit der Protokolldaten zur Verfügung.
M 6.151	Alarmierungskonzept	Ein Alarmierungskonzept ist auf Basis von Benutzergruppen, Rollen und Alarmierungsregeln umsetzbar.

4. VON DER THEORIE IN DIE PRAXIS: DATENSCHUTZ VERSTÄNDLICH GEMACHT



Allen Anforderungskatalogen mit gesetzlichen Rahmenbedingungen zum Trotz: Dieses Whitepaper hat nicht den Anspruch einer juristischen Aufklärung, denn auch die Autoren sind keine Rechtsexperten. Aus der Praxis zeigt sich jedoch, dass Fachkenntnisse aus der IT sowie der Organisation sehr nützlich sein können, sich dem Thema anzunähern. Sichtbar wird das auch an der Tatsache, dass es viel mehr die Datenschutzbeauftragten denn die Juristen eines Unternehmens sind, die sich mit dem Datenschutzgesetz und der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) auseinandersetzen. Dies ist auch in der täglichen Praxis hilfreich, denn hier kann wichtiger Input folgen.

Zweifellos sind auch Mechanismen und Hard- sowie Software-Lösungen notwendig, um die gesetzlichen Vorgaben zu erfüllen. Neben Türschließsystemen (Zutrittskontrolle) und konkret vorgeschriebenen Produkten wie einer Verschlüsselungs-Software ist in den einschlägigen und als Referenz angeführten Gesetzestexten sowie Erläuterungen bzw. in empfohlenen Maßnahmenkatalogen (BSI, ISO u.a.) auch die Protokollierung und Zugriffskontrolle explizit und in prominenter Rolle erwähnt.

4.1. „EU first" – die Rahmenbedingungen der EU-DSGVO

Mittlerweile ist die DSGVO in unserem beruflichen Alltag angekommen. Informationsveranstaltungen und Internet-Recherchen geben einen Überblick, jedoch ist der Schritt zu einer umfassenden Beratung oft noch nicht gemacht. Gründe für Nicht-Aktivität gibt es immer, in Vorleistung zu gehen für eine unbestimmte Rechtslage ist für viele kein Thema. Dies kann Unternehmen aber teuer zu stehen kommen, denn die Rechtslage ist mit der EU-DSGVO eigentlich geschaffen.

Umstände, die es zu berücksichtigen gilt, sind:

- Europäisches Recht ist nun umsetzbar. Das bedeutet einen Paradigmenwechsel in Datenschutz und IT-Security hin zum anglikanischen Rechtssystem. Wir erinnern uns, dass auch Kartell- und Finanzstrafen sowie Strafzahlungen, veranlasst durch die FMA, in die Millionen steigen können. Die EU setzt auf das Prinzip „Datenminimierung, Datenschutz und IT-Security", um nach den Erkenntnissen aus den Spionage-Fällen der NSA und der damit einhergehenden globalen Dominanz der US-Software-Konzerne ein neues Geschäftsmodell für die europäische Industrie zu finden. Weitere Gründe dürften auch hohe Strafzahlungen der US-Konzerne sein, ebenso die Durchbrechung der Steuerflucht in Steueroasen. Sozusagen „EU first", denn hier sollen Software-Unternehmen und Cloud-Anbieter für Arbeitsplätze, höhere Security-Standards und eben einen kontrollierbaren Datenschutz für Bürger und Kunden sorgen[1].

[1] https://www.heise.de/newsticker/meldung/Deutsche-Konzerne-bauen-Datenplattform-gegen-Google-Co-3705594.html

- Nicht zu vergessen ist das österreichische Spezifikum, dass nun eine Thematik relevant wird, die bisher keine Bedeutung hatte, wenn man von internationalen Konzernen absieht. Governance, Compliance und Datenschutz oder Datensammlungen für forensische Analysen waren bisher aus verschiedenen Gründen kein Thema und die Strafen für Verstöße waren symbolisch.

- Soziale Medien („Shitstorms"), Fachanwälte („Abmahnspezialisten") und internationale Behörden und Gerichte stellen eine unkalkulierbare Macht dar, mit denen eigentlich jederzeit zu rechnen ist. Nationale Datenschutzbehörden verstärken die Kooperationen und geben Kompetenzen ab, um Verfahren zu konzentrieren („One-Stop-Shop")[2]. Internationale Prozesse bis hin zum EUGH in der Letztinstanz werden die Regel, die Kosten und Aufwände dafür steigen astronomisch.

EXKURS: Ein Überblick über die Lage in Österreich

Das System der Datenschutzbeauftragten (DSBa) wurde in Österreich durch die DSGVO neu eingeführt. Die Regelungen, ob ein DSBa benötigt wird, sind in manchen Fällen vage, in Spezialfällen obligatorisch (Kreditschutz- und Finanzauskunfts-Unternehmen). Hier hilft ein Blick über die Grenzen nach Deutschland. Die Grenzfälle sind auf jeden Fall gut beraten, einen DSBa zu bestellen. Das EU-Recht brachte uns folgende Neuerungen:

- Beweislastumkehr
- Entschädigung auch immaterieller Schäden
- Wahl des Gerichtsortes
- hohe Bußgelder mit „abschreckender Wirkung"

Nichtgewinnorientierten Vereinen und Verbänden (NGO) ist es nun teilweise möglich, sich um Kunden- und Bürgerinteressen zu kümmern[3].

[2] https://www.datenschutz-notizen.de/datenschutz-grundverordnung-aufsichtsbehoerden-one-stop-shop-1214799/
[3] https://www.golem.de/news/dsgvo-amazon-bekommt-746-millionen-euro-datenschutz-strafe-2107-158564.html

4.2. Datenschutz-Folgeabschätzung bei erhöhtem Risiko

Besteht eine erhöhte Gefahr, dass persönliche oder gar sensible Daten öffentlich und somit Datenschutzrechte der höchstpersönlichen Dateneigentümer (nicht zu verwechseln mit den Datenverwendern oder -inhabern) verletzt werden, ist eine Risikoabwägung durchzuführen und zu dokumentieren. Daraus sind die Schlüsse zu ziehen, die Gefahrenmatrix regelmäßig abzutesten sowie wiederum Gefahrenpotenziale zu minimieren.

Das Gebot nach technischem Stand und Verhältnismäßigkeit kann berücksichtigt werden, das Endergebnis dieser Abwägungen stellt jedoch der Richter im Prozess. Generell würde sich also ein Assessment empfehlen, das monatliche Reports und Grafiken zum Stand der Systeme abbildet. Log Management in Verbindung mit einem Schwachstellen-Scanner wäre somit mehr als empfehlenswert – und arbeitserleichternd.

4.3. Risikogruppen per Definition – Städte, Gesundheitssektor und Profiler

Bemerkenswert ist auch die Tatsache, dass vor allem im öffentlichen Bereich der größte Handlungsbedarf besteht, ausgerechnet hier aber die Verantwortlichen den geringsten Bedarf sehen. In Gemeinden und Städten ergibt sich dieser Zusammenhang aus den vielschichtigen Rollen- und Funktionärskompetenzen, die sich vermischen und in vielen Fällen für Konflikte sorgen werden.

Die Rolle des Vereinsmitgliedes, des politischen Mandatsträgers und des Gemeindebediensteten ist oft in einer Person zu finden. Die Fußballmitgliederdaten, die Feuerwehrspenderliste und die nächste Wahlaussendung-Adressdatei werden vermischt – eine Excel-Liste erzeugt neue Daten. In den Augen des Erfinders „gehört" diese aktuelle Datei sogar ihm persönlich und wird nur zu oft in gefälliger Weise weitergegeben.

Werden dann noch sensible Daten über Gewerkschaftszugehörigkeiten oder gar religiöse Bekenntnisse weitergegeben – oder sind leicht wiederherstellbar –, vielleicht sogar noch (irrtümlich) an alle versendet, stellt dies einen Datenschutz-Supergau dar, der sehr teuer sein kann. Geo-Daten, biometrische und gesundheitliche Daten sind ebenso höchst schutzbedürftig wie sexuelle oder politische Präferenzen und Datensätze, die eine Existenz oder oft viele Tausende sozial und/oder finanziell ruinieren können.

Big-Data-Sammler sollten zudem für höchste Prozesstransparenz sorgen, indem dokumentiert ist, wer wo zugreifen darf und in welchem Auftrag er handelt. Überdurchschnittliche IT-Sicherheitssysteme werden verlangt – bei Nicht-Einhaltung oder einem Data-Breach unter fahrlässigen Bedingungen wird z. B. der Investor sehr rasch wieder aus dem Start-up abspringen – wie auch die betroffenen Kunden.

4.4. Zwei Datenschutz-Themen, die nur technisch zu lösen sind

Das Prinzip der **Datenminimierung** ist vorgeschrieben – nach Ablauf der gesetzlichen Fristen der einzelnen Datenkategorien (Buchhaltungsdaten: 7 Jahre; Zeugnisse: bis 30 Jahre etc.) sollten Daten vernichtet werden. Alle weiteren Daten, deren Aufbewahrung nicht extern reguliert ist, sollten gemäß Löschkonzept vernichtet werden, je früher umso besser.

Somit kommt diesem Thema eine besondere Bedeutung zu – und zwar in Verbindung mit Awareness und eigenverantwortlichem Handeln der Datenverarbeiter, sprich der Mitarbeiter und Verantwortlichen. Es ist jedem, der Daten verarbeitet, versendet oder löscht, anzuraten, den Vorgang zu überdenken. Zu oft sind sicherheitsrelevante Vorfälle der Tatsache geschuldet, dass „lustige oder vollkommen unnötige" Handlungen durchgeführt werden. So häufen sich bereits Beschwerden bei der Datenschutzbehörde von Kindern über ihre Eltern – Stichwort „Facebook".

Insbesondere für archivierte Daten gelten zudem die **Pseudonymisierung** und **Anonymisierung** als explizit erwähnte Methoden, wenn diese noch für statistische Zwecke verwendet werden. Daten, die persönliche und sensible Inhalte haben, aber auch geheime Daten aus Produktion, Forschung und Entwicklung sowie aus der Finanzwelt haben in der Öffentlichkeit nichts verloren und sollten unbedingt verschlüsselt werden. Daten in Cloud-Speichern[4] aus Drittländern (USA, Asien etc.) müssen verschlüsselt übertragen, dort gelagert und rückgeführt werden. Empfehlenswert sind auch Trennungen in private und berufliche „Container" auf Smartphones. WhatsApp ist übrigens nicht datenschutzkonform.

[4] https://www.infopoint-security.de/gemalto-studie-datensicherheit-in-der-cloud-bereitet-unternehmen-probleme/a8361/

5. LOG MANAGEMENT: I'LL BE BACK!

Das zweite große Element ist zweifellos das Log Management mit Security Event- & Information-Management-Fähigkeiten.

In den letzten Jahren war Log Management das wohl unbeliebteste Thema in der IT: Komplexe Zusammenhänge, teure Datenspeicherung und hoffentlich nie notwendige Forensik waren zu schwache Argumente für die oft hochpreisige Anschaffung. Jene Institutionen und Konzerne, die sich dennoch dafür entschieden haben, sind mit Sicherheit in Gedanken längst bei der Ablösung des Tools oder haben dieses nicht mehr aktiv in Verwendung.

Die neuen Trends in der Digitalisierung bewirken aber gerade einen massiven Umschwung. Governance und Compliance sind nicht mehr die Triebfedern für eine Anschaffung, sondern

- explizite Protokollierungserfordernisse in den Datenschutzgesetzen (DSG, BDSG, EU-DSGVO),
- jeder Standard (PCI DSS, BSI, ISO usw.) empfiehlt das Sammeln von Logs und Aktivitäten,
- Log Management konsolidiert gesamte IT zu einem ISMS,
- SIEM ermöglicht eine echtzeitnahe, flexible Erkennung und Abwehr laufender Angriffe,
- flexible Preismodelle und Managed-Security-Services für einen kalkulierbaren Invest,
- Integration von Produktionsumgebungen, IoT, smarten Anwendungen in Datacenter-IT
- und viele weitere mehr.

Neben konkreten Erfordernissen, die sich vor allem im Artikel 32[5] der EU-DSGVO wiederfinden, sprechen vor allem praktische Erfordernisse für eine Log-Management-Lösung.

Diese wären unter anderem:

a.) Das Erbringen einer **Datenschutz-Folgeabschätzung** ist für viele größere, in risikobehafteten Branchen tätige Unternehmen und Institutionen notwendig. Somit wird eine Risikomatrix erstellt, wobei man sich natürlich die Frage stellen muss, welche objektiven Kriterien dafür vorliegen. „Failed Logins" von Mitarbeitern sollten dokumentiert werden, um die Neugierde der Mitarbeiter auch beurteilen zu können. Wer greift unberechtigt auf Forschungsdaten zu, die eigentlich geschützt sein sollten? Das Rating von Gefahren und die Einschätzung der Angriffsmuster kann nur sinnvoll abgebildet werden, wenn Alarme, Reports und Meldungen vorliegen.

b.) Der **Datenschutzbeauftragte** wird umfassendes Reporting- und Analysematerial einfordern. Bei einem meldepflichtigen „Data Breach" ist er auch der Ansprechpartner der Datenschutzbehörde. Er wird seine Verantwortlichkeit nachweisen müssen, ebenso die im Endeffekt haftende Geschäftsführung. Ohne ein Security-Management-System und „nur" auf einige Firewallreports hoffend, wird es wohl teuer werden. Ein guter Perimeter-Schutz ist mittlerweile nicht ausreichend, denn die meisten Vorfälle passieren aufgrund von Missverständnissen, Fehlern und mutwilligen Aktionen seitens Mitarbeitern oder Angreifern, für die Anti-Viren-Lösungen und auch Next-Generation-Firewalls nicht ausreichen.

[5] https://dsgvo-gesetz.de/art-32-dsgvo/

c.) **Big Data** ist mehr als ein Schlagwort. In jedem Krankenhaus, in jeder Gemeinde oder auch bereits in „kleinen Start-ups“ werden riesige Mengen an Daten erhoben, gespeichert, verändert, gelöscht, Profile erstellt oder neue Datenkategorien erzeugt. Genetische Daten, Befunde, Bankdaten oder Lebensläufe und Informationen aus sozialen Medien ermöglichen neue Geschäftsmodelle und somit auch Gefahren. Das Prinzip „Wer hat wann worauf und warum“ zugegriffen, gilt auch hier. Werden Daten gelöscht, verändert und einfach nur unbefugt angesehen, liegt bereits ein Verstoß vor, der mediengerecht aufbereitet und prozessual gesehen sehr kostspielig werden kann.

d.) Ein **Besuch vom Amt** ist bisher schon üblich gewesen, dieser wird aber wohlweislich diskret abgehandelt. Man hat noch nie gehört oder gelesen, dass sich ein Unternehmen oder eine Institution damit rühmte, von der Datenschutzbehörde besucht und für einwandfrei „datenschutzkonform“ erklärt worden zu sein. Laut österreichischem Datenschutzbericht wurden im Jahre 2020 337 amtswegige Prüfverfahren durchgeführt, das sind fast so viele wie 2018 und 2019 zusammen.

Fehlerquellen und beanstandete Sicherheitslücken sind in vielen Fällen und auch branchenunabhängig zu sehen: Die Videoüberwachung löst immer Bedenken aus und ist umfassend geregelt, aber ebenso die Datenzugriffe nicht autorisierter Personen, ob aus Neugierde, Eigennutz oder aus politischen oder persönlichen Gründen. Es genügt auch bereits die Einsichtnahme in diese Daten, ohne diese kopieren, versenden oder löschen zu wollen.

5.1. Gesetzliche Grundlagen für den Einsatz einer Log-Management-Lösung

5.1.1. Österreich

In Österreich sieht das Datenschutzgesetz eine klare Aussage zur Protokollierung bei einer Bildverarbeitung im Paragraf 13[6]:

(2) Der Verantwortliche hat – außer in den Fällen einer Echtzeitüberwachung – jeden Verarbeitungsvorgang zu protokollieren.

(3) Aufgenommene personenbezogene Daten sind vom Verantwortlichen zu löschen, wenn sie für den Zweck, für den sie ermittelt wurden, nicht mehr benötigt werden und keine andere gesetzlich vorgesehene Aufbewahrungspflicht besteht. Eine länger als 72 Stunden andauernde Aufbewahrung muss verhältnismäßig sein und ist gesondert zu protokollieren und zu begründen.

Eine weitere Erwähnung der Protokollierung erfolgt im 3. Hauptstück (§ 50), hier wird konkret Protokollierung für die Verarbeitung strafrechtlicher Daten im Bereich polizeilicher Staatsschutz und Maßnahmenvollzug gefordert.

[6] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597

Andere Erwähnungen, die bisher im DSG 2000 vorhanden waren, wurden im DSG gestrichen (Treu und Glauben, Zweckbindung, Verantwortung), da diese bereits durch die DSGVO gelten.

Eine weitere Erwähnung erfolgt im Forschungsorganisationsgesetz (§ 2d (1) 1. FOG), auch hier wird eine lückenlose Protokollierung der Verarbeitung personenbezogener Daten gefordert.

Abschließend ist festzustellen, dass die österreichische Datenschutzbehörde seit mehreren Jahren Schwerpunktkontrollen durchführt und besonders im Gesundheitssektor[7] auf das Thema Protokollierung achtet. Unberechtigte Abfragen über Gesundheitsdaten und zu wissbegierigen Mitarbeitern soll ein Riegel vorgeschoben werden. In der RIS-Rechtsdatenbank[8] finden sich unter dem Stichwort „DSB" viele Einträge, Erkenntnisse und Empfehlungen der Datenschutzbehörde.

Mit einer Log-Management-Lösung können, als unbestreitbaren Vorteil, punktgenau Security-Anforderungen eingepflegt werden, die von den Verantwortlichen gefordert sind. So könnte man aus dem Windows Active Directory (Berechtigungs-Management) jede Neuanlage eines Mitarbeiters automatisch melden. Dieser Vorgang ist zumeist Routine, jedoch auch von Hackern gerne genutzt, wenn sie sich bereits im internen Netz befinden. Die Alternative wäre die Anschaffung eines spezifischen Tools, das sich auf das Management und Reporting des Berechtigungsschemas fokussiert.

In seinen Kernfunktionen ist es die Aufgabe einer Log-Management-Software, Zugriffe zu erlauben oder zu verweigern, die Logs über diese Vorgänge zu archivieren, um sie einer späteren forensischen Analyse gerichtsfest zuzuführen. Log Management kann unter anderem Anwendungen generell erlauben oder versagen, wodurch Missbrauch erst gar nicht ermöglicht wird. Mandantenfähigkeit lässt außerdem zu, dass über Unternehmensbereiche und Konzernstrukturen hinweg die Rollen eindeutig zu vergeben sind. So können zum Beispiel auch vergebliche Passwort-Eingaben überwacht und dann gemeldet werden. Durch die offene Architektur geht Log Management weit über herkömmliche Security-Tools hinaus und sieht sich als zentrales System, das Logs aus vielen Quellen konsolidiert, Handlungen erlaubt und auch via E-Mail alarmiert.

[7] https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=b7ff4838-a52a-456c-998b-4c9e4732c1f4&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=&Norm=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20170201_DSB_D213_469_0006_DSB_2016_00

[8] https://www.ris.bka.gv.at/

5.1.2. Deutschland – Bundesdatenschutzgesetz

In Deutschland ist das Bundesdatenschutzgesetz[9] sehr deutlich und regelt in Paragraf 76 die Protokollierung wie folgt:

(1) In automatisierten Verarbeitungssystemen haben Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren:
1. Erhebung,
2. Veränderung,
3. Abfrage,
4. Offenlegung einschließlich Übermittlung,
5. Kombination und
6. 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.

(4) Die Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen.

(5) Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle der oder dem Bundesbeauftragten auf Anforderung zur Verfügung zu stellen.

Wo hier die Reise hingeht, kann man auch an der Stellungnahme des Datenschutzbeauftragten des Landes Mecklenburg-Vorpommerns aus dem Januar 2017 erkennen:

„Vielmehr beschränkt sich die Vorschrift auf die **Protokollierung** der Zugriffe der Nutzerinnen und Nutzer. In § 76 Abs. 1 sollte explizit festgelegt werden, dass auch administrative Vorgänge (z. B. Löschläufe, Datenbankzugriffe, Erstellung von Backups) zu protokollieren sind, da diese unter Umständen einen weit größeren Einfluss als einzelne Verarbeitungsvorgänge haben. Darüber hinaus ist eine automatische Protokollierung der Datenübertragung an Schnittstellen von Verfahren zu anderen Verfahren erforderlich. Schließlich sollten Aufbewahrungsfristen für Protokolldaten geregelt werden. In Bezug auf die Protokolldaten für einzelne Verarbeitungsvorgänge ist es sinnvoll, Protokolldaten ebenso lange wie die gespeicherten Daten aufzubewahren.“

[9] https://www.gesetze-im-internet.de/bdsg_2018/

5.1.3. Europa – EU-DSGVO

Die EU-DSGVO sieht an mehreren Stellen vor, dass durch **technisch-organisatorische Maßnahmen** bereits im Vorfeld einer Datenabfrage dafür gesorgt wird, dass der Datenverarbeiter lediglich jene Daten und Informationen erhält, für die er befugt ist. Wir denken hier insbesondere an Krankenhäuser, wo Ärzte und Pflegepersonal durch Voreinstellungen in der Software nicht die Möglichkeit haben, Gesundheitsdaten abzufragen, für die sie nicht autorisiert sind.

Neben dem Logging der Aktivitäten sind auch Löschkonzepte bzw. das zeitliche Ablaufen von Zugriffsrechten vorzusehen. Wollen diese wiedererlangt werden, sind freie Begründungsfelder oder die explizite Vorgabe anzudenken, das Zugriffsrecht erneut anzufordern. Der Artikel 25 in der EU-DSGVO regelt derartige Sachverhalte so, dass durch **„Technikgestaltung und Voreinstellungen"** eine derartige Software vorausgesetzt wird. In den meisten Fällen wird dies durch spezifische Krankenhaus-Management-Systeme abgebildet, jedoch bilden diese Spezialanwendungen keine Insellösungen, sondern es werden wohl viele verschiedene Systeme (Datenbanken, Windows, Excel etc.) übergreifend genutzt.

Ähnliche Sachverhalte ergeben sich aus CRM- und ERP-Software-Lösungen, wo mit Sicherheit persönliche und auch sensible Daten abgelegt werden. Auch diese Anwendungen sollten in eine Log-Management-Lösung eingebunden werden.

Artikel 25 (2)[10] besagt nun wie folgt:

Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

[10] https://www.datenschutz-grundverordnung.eu/grundverordnung/art-25-ds-gvo/

6. PROGNOSE – BEISPIELE VON DATENSCHUTZ-SUPERGAUS

a.) HR-Management

Sie bedienen sich als Unternehmen einer Recruiting-Plattform, die das Bewerber-Management in der Cloud und als mobile Lösung anbietet. Diese wiederum hostet die Daten in einem Rechenzentrum in einem Drittland. Bereits das Fehlen eines gut verhandelten Dienstleistervertrags mit der Jobbörse ist ein schwerwiegender Mangel. Wenn dann zwischen Auftragsdatenverarbeiter und dem z. B. amerikanischen Rechenzentrumsdienstleister auch keine datenschutzrechtlichen Vereinbarungen vorliegen, haben rechtlich gesehen alle einen schweren Stand.

TIPP: Datenminimierung beim Bewerber-Management. Ehestmöglich alle Daten löschen und strengste Vertraulichkeit und rechtliche Absicherung mit Projektpartnern (Jobhunter, Jobbörsen, Mitarbeitern). Die Einwilligung vom Bewerber einzuholen, falls die Daten länger gespeichert werden, ist verpflichtend. Im Idealfall werden diese mit der Absage gelöscht.

b.) Social Hacking dank organisatorischer Schwächen

Ob unzählige „CIO-Fraud"-Beispiele, Online-Banking-Betrug dank gefälschter E-Mails oder gar physisches Eindringen in ein Gebäude, das wegen einer laxen Zutrittskontrolle nicht bemerkt wird, sind die Regel, nicht mehr die Ausnahme.

Ob dahinter Cyber-Kriminelle, Industriespione oder Agenten fremder Mächte stecken ist eigentlich nebensächlich, denn der Schaden ist enorm. Insbesondere E-Mails und sehr gut gemachte Fake-Anrufe können dafür sorgen, dass persönliche Daten gestohlen und missbraucht werden. Institutionelle Schwachstellen wie fehlende Schulungen oder ausgiebig verteilte (Admin- oder) Zugriffsberechtigungen sorgen dafür, dass vertrauliche Daten unbemerkt außer Haus gelangen. Gute Pen-Tester mit falschen Identitäten, aber richtig gutem schauspielerischem Geschick, gelangen bis in die Vorstandsetage oder in gesicherte Serverräume.

TIPP: Die Entwicklung einer Firmenkultur, die auch auf Sicherheit bedacht ist, ist von entscheidender Bedeutung. Achtlosigkeit und Unbekümmertheit führt in Zukunft zu massiven Problemen.

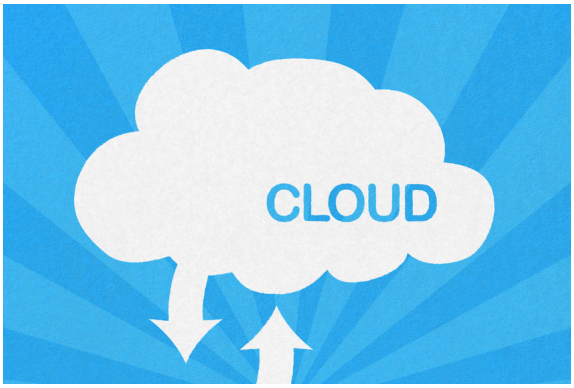
c.) Potpourri des Grauens: Smartmobile-Cloud-Fabrik

Waren bisher zwei Welten, die Office-IT und die Produktion, relativ getrennt, entstehen nun Geschäftsmodelle und Angebote, die eine Spur des Datenschutz-Grauens ermöglichen. Ein Beispiel ist der Trojaner-verseuchte USB-Stick, der dann vom Laptop sensible Daten herunterlädt oder Schadcode auf den Systemen verteilt.

Fehlende Prozesse, mangelndes Know-how und Unbekümmertheit sorgen bereits für aufsehenerregende, unzählige Beispiele in den Medien: Die sprechende Barbie oder der spionierende Teddybär lassen grüßen.

d.) Blindes Vertrauen in die Welt des Guten

Das Internet ist für sehr viele Vorteile und Annehmlichkeiten bekannt, ist aber auch ein Vehikel für Schwerkriminelle, vermeintlich sozial Benachteiligte und Menschen mit der einen oder anderen Charakterschwäche. Es herrschen Syndikate, Einzelpersonen und Organisationen aller Art im Darknet und in anderen Untiefen des Netzes. Aber auch die Marketing-Abteilungen der Konzerne versprechen das Blaue vom Himmel, das leider niemandem vor Gericht hilft.



Ein Beispiel dafür, dass oft die linke Hand nicht weiß, was die rechte macht, sei hier dargestellt: Facebook bestreitet im Jahr 2019 500 Millionen Zugangsdaten offengelegt zu haben, war sich aber nicht sicher genug, als dass es seine User nicht zu einem Passwort-Wechsel aufforderte.

7. ABSCHLUSSBEMERKUNG

Mittlerweile haben auch die Datenschutzbehörden und selbst die Gerichte ein neues Selbstbewusstsein erfahren und scheuen auch nicht davor zurück, Urteile zu fällen, die für die internationalen Konzerne sehr kostspielige Folgen haben. Bis vor kurzem war es kaum vorstellbar, dass die Rechtsansichten der „Multis" angezweifelt und selbst einfach zu erledigende Vorgänge wie das Löschen von Hass-Postings auf Anfrage einen riesigen Aufwand[11] verursachen würden.

In großen Organisationen steht die eigene Existenzberechtigung und Prosperität immer im Vordergrund. Aus diesen Gründen ist dem Führungspersonal dringend zu empfehlen, die Aktivitäten der Mitarbeiter, unternehmensfremder Personen und auch der Stakeholder zu dokumentieren, um sich abzusichern. Dies erzwingt eine Protokollierung der Tätigkeiten, eine genaue Definition der Prozesse und Aktivitäten sowie eine „Kultur der Security-Awareness". Es sei angeraten, sich bei der Protokollierung nach einer europäischen Software umzusehen, um nicht das Feuer mit Öl zu bekämpfen.

Die Erfahrung zeigt, dass ein sinnstiftendes Tool für Log Management und Forensik mehrere starke Komponenten umfasst, die bedacht werden sollten:

- personalintensives und hohes Know-How erfordernd, wodurch eine Managed-Service-Variante empfehlenswert ist
- hohe Integration in die individuelle, bestehende IT-Landschaft notwendig
- hohe Beratungskompetenz des Projekt-Teams erforderlich
- Fokus auf Investitionsplanung und Kostensicherheit (Lizenzierungsverfahren)
- hohes Level an Prävention, Abwehrkraft und Angriffserkennung erhöht die Überlebensfähigkeit des Unternehmens
- mehrere Ziele und Mehrwerte definieren, z. B. Datenschutz, Security, Forensik, IoT-Integration etc.

Im Sinne der Bürger- und Verbraucherrechte ist ein strenges Datenschutzregime sehr zu begrüßen. Selbst wenn Daten öffentlich werden, besteht zumindest eine Aussicht auf Genugtuung, Schadenersatz und eine Verbesserung in der Zukunft.

[11] http://www.oe24.at/digital/Gruene-zwingen-Facebook-in-die-Knie/281733491

8. Anhang

8.1. BSI

Baustein, Maßnahme	Link
B 5.22 Protokollierung	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05022.htm
M 2.110 Datenschutzaspekte bei der Protokollierung	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02110.html
M 2.496 Geregelte Außerbetriebnahme eines Protokollierungsservers	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02496.html
M 2.497 Erstellung eines Sicherheitskonzepts für die Protokollierung	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02497.html
M 2.499 Planung der Protokollierung	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02499.html
M 2.500 Protokollierung von IT-Systemen	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02500.html
M 2.64 Kontrolle der Protokolldateien	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02064.html
M 3.89 Schulung zur Administration der Protokollierung	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03089.html?nn=6610630
M 3.90 Allgemeine Grundlagen für die zentrale Protokollierung	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03090.html
M 4.47 Protokollierung der Sicherheitsgateway-Aktivitäten	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04047.html
M 4.225 Einsatz eines Protokollierungsservers in einem Sicherheitsgateway	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04225.html
M 4.227 Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04227.html
M 4.430 Analyse von Protokolldaten	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04430.html
M 4.431 Auswahl und Verarbeitung relevanter Informationen für die Protokollierung	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04431.html
M 5.171 Sichere Kommunikation zu einem zentralen Protokollierungsserver	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05171.html
M 5.172 Sichere Zeitsynchronisation bei der zentralen Protokollierung	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05172.html
M 6.151 Alarmierungskonzept für die Protokollierung	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m06/m06151.html

Bildnachweise

Seite 2: The concept of technology, the Internet and the network. Businessman shows a working model of business: Protect your data © photon_photo / fotolia.com
Seite 11: Businesswoman Signing Into Website On Laptop © Andrey Popov / fotolia.com
Seite 11: European Union flag against European Parliament © artjazz / fotolia.com
Seite 13: Überweisungsschein und Gesundheitskarte © Jürgen Fälchle / fotolia.com
Seite 16: Statue of justice © sebra / fotolia.com
Seite 17: 3D Illustration Map Outline of Austria with the Austrian Flag © Fredex / fotolia.com
Seite 19: Anwendung/Einführung der Datenschutz-Grundverordnung und damit Ende des Bundesdatenschutz-Gesetzes © n8aktiver / fotolia.com
Seite 20: 3D Cell Smart Phone with Envelope © Fenton / fotolia.com
Seite 20: bewerbungsgespräch - © contrastwerkstatt / fotolia.com
Seite 21: Policies and Procedure. Two binders on desk in the office. Busin © tumsasedgars / fotolia.com
Seite 21: Cloud © John Smith / fotolia.com

Über die iQSol GmbH

Die iQSol GmbH setzt seit Gründung 2011 auf die Entwicklung und Bereitstellung von IT-Security-Lösungen, die die IT-Infrastruktur von Unternehmen absichern, für einen reibungslosen Betrieb sowie ein unterbrechungsfreies Arbeiten sorgen. Die Lösungen aus den Bereichen Alarmierung, Log und Power Management sind bei Kunden verschiedener Branchen in Österreich, Deutschland sowie Osteuropa im Einsatz.

Die Autoren

Jürgen Kolb ist Managing Partner der österreichischen iQSol GmbH. Nach verschiedenen beruflichen Stationen sowohl in der öffentlichen Verwaltung als auch im Privatsektor gründete er als (fast fertig studierter) Wirtschaftswissenschaftler gemeinsam mit DI Alexander Graf das Unternehmen.

Heute verantwortet Jürgen bei der iQSol GmbH den Bereich Sales, PR & Marketing und Finanzen. iQSol ist seine zweite erfolgreiche Unternehmensgründung, denn auch am Aufbau der Antares NetlogiX Netzwerkberatung GmbH ist er schon seit Beginn im Jahr 2001 beteiligt und fokussiert sich auf das Thema Datenschutz und IT Organisation.

Dr. Wolfgang Zuser ist IT-Projektmanager und IT-Architekt mit ganzheitlicher, benutzerorientierter und stets lösungsorientierter Herangehensweise. Er verfügt über 15 Jahre breit gestreute Erfahrung von IT-Infrastruktur- bis zu Anwendungsentwicklungsprojekten sowie Managementberatung.

Bei iQSol ist Wolfgang Zuser für das Produktmanagement und die Entwicklungsleitung von LogApp verantwortlich.

iQSol GmbH
Petrusstraße 20
A - 3312 Oed

T: +43 7472 207 67
E: office@iqsol.biz

www.iqsol.biz