ENGINSIGHT

ISMS NACH ISO 27001 UMSETZEN

Effektiv mit ENGINSIGHT

ENGINSIGHT
MEHR ALS EINE CHECKLISTE

Ein Informationssicherheitsmanagement (ISMS) etablieren und betreiben – ohne technisch gestützte Verfahren? Ein Ding der Unmöglichkeit. Während die Kontrolle organisatorischer Maßnahmen auf manuelle Checklisten angewiesen ist, können Sie technische Controlls mit Enginsight automatisieren.

ISMS mit ISO 27001

Zwei Standards liefern branchenunabhängige Vorgaben zur Steigerung des IT-Sicherheitsniveaus. Einerseits die nationale Norm des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit dem IT-Grundschutz. Andererseits die international gültige Norm ISO/IEC 27001. Während der IT-Grundschutz sehr formalistische und präzise Vorgaben macht, bleiben in der ISO 27001 bewusst Spielräume, um eine individuelle Umsetzung und Anpassung an technische Innovationen zu ermöglichen.

Die ISO 27001 legt den Fokus auf eine vollständige Risikoanalyse. Das ISMS hilft Ihnen dabei, Prozesse zu reflektieren und Risiken zu identifizieren, um daraus Folgemaßnahmen abzuleiten und umzusetzen.

IT-Risiken mit Enginsight analysieren

Mit Enginsight gelingt der Aufbau und das Erfüllen der technischen Anforderungen aus der ISO 27001. Im Gegensatz zu einfacher Checklisten-Software sammelt Enginsight automatisiert Daten zum Sicherheitszustand Ihrer IT-Assets. Durch die automatisierte Inventarisierung stellen sicher, dass keine IT-Assets vergessen werden und keine Schatten-IT im Anwendungsbereich Ihres ISMS entsteht. Die Automatisierungsmöglichkeiten in Enginsight schaffen noch weitere Vorteile:

- ✓ Die Ergebnisse bleiben unabhängig von der Tagesform des Testers.
- ✓ Der Arbeitsaufwand und die Kosten sind deutlich reduziert.
- ✓ Dank eindeutigem Scoring erhalten Sie einen wichtigen Anker für fundierte Risikoanalyse.
- ✓ Die gewonnene Zeit können Sie nutzen, um sich auf die organisatorischen Maßnahmen zu fokussieren.

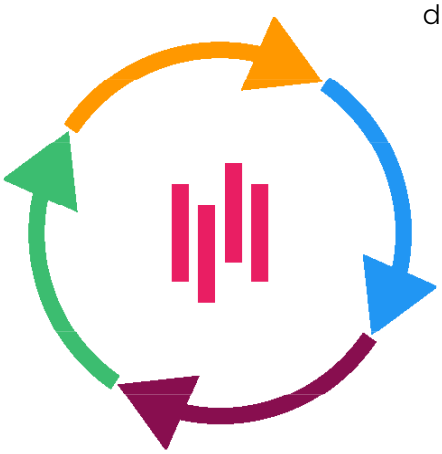
Führende Norm für IT-Sicherheit: ISO/IEC 27001

- ✓ Weltweit anerkannter Standard
- ✓ Internationaler Wettbewerbsvorteil
- ✓ Offen für technologischen Fortschritt
- ✓ Flexible Anpassung an individuelle Risiken, Bedürfnisse und Ressourcen
- ✓ ISMS schafft einen Überblick der IT-Infrastruktur
- ✓ Relativ schnelle Implementierung
- ✓ Risikobasiert

GEMEINSAM SICHERHEIT SCHAFFEN
IN EINER DIGITALEN WELT

In **regelmäßigen und geplanten Abständen** durchgeführte interne Audits zum Sicherheitszustand Ihrer IT-Infrastruktur stellen ein Kernstück der ISO 27001-Norm dar. Bei der Einführung der Norm gleichen Sie Ist-Zustand des Informationssicherheitsmanagements mit den Vorgaben der ISO 27001 ab. Anhand der Audits wird regelmäßig überprüft, ob die Anforderungen aufrechterhalten werden oder Abweichungen vorliegen.

So können bei möglichen Fehlentwicklungen schnell entsprechende Gegenmaßnahmen eingeleitet werden. Wichtig ist hierbei, dass die wiederholten Risikobeurteilungen stets **konsistente, gültige und vergleichbare Ergebnisse** liefern.



Auf den Prüfstand kommen bei einem Audit ebenso die organisatorischen wie technischen Maßnahmen, deren Überprüfung in einem Auditplan zuvor definiert wird. Enginsight bietet enorme Potenziale, um zentrale Elemente der Audits zu automatisieren. Die Bereiche **Assetmanagement und Betriebssicherheit** sind hierbei hervorzuheben. Erstellen Sie mit Enginsight **Vorlagen für automatisierte Penetrationstests**, die wiederkehrend und zur gewünschten Zeitpunkt durchgeführt werden. Als Datengrundlage für die Zielsysteme dient die **automatisierte IT-Inventarisierung**, die alle IP-Adressen im Firmennetzwerk sammelt und kategorisiert.

Ein **eindeutiges Scoring** der Ergebnisse ermöglicht es Ihnen, die aufgespürten Sicherheitsrisiken zu bewerten und Maßnahmen zur Risikobehandlung zu priorisieren. Mit Enginsight kennen Sie einfach Nichtkonformitäten und leiten, wenn nötig, Korrektureen ein.

Zu Dokumentationszwecken und als Nachweis können Sie sich die **Ergebnisse des Audits als PDF-Bericht** ausgeben lassen.

Die Vorteile gegenüber einer manuellen Ausführung sind vielfältig:

- ✓ Sie stellen sicher, dass neue IT-Assets nicht vergessen werden und keine Schatten-IT im Anwendungsbereich Ihres ISMS entsteht.
- ✓ Die Ergebnisse bleiben unabhängig von der Tagesform des Testers.
- ✓ Der Arbeitsaufwand und die Kosten sind deutlich reduziert.
- ✓ Dank eindeutigem Scoring erhalten Sie einen wichtigen Anker für die Risikobewertung.

REFERENZMAßNAHMENZIELE NACH ISO 27001/27002

Über 100 Referenzmaßnahmenziele gibt die ISO 27001 bzw. ISO 27002 vor. Die lange Liste an Anforderungen mag auf den ersten Blick erschlagend wirken. Eine Vielzahl zentraler Maßnahmen lassen sich jedoch mit Enginsight umsetzen oder unterstützen.

MAßNAHME	FUNKTIONEN IN ENGINSIGHT, DIE IHNEN HELFEN, DIE ENSPRECHENDE MASSNAHME UMZUSETZEN
5. ORGANISATORISCE MASSNAHMEN	
5.2 Informationssicherheits-rollen und -verantwortlich-keiten	Enginsight ermöglicht das Zuweisen von Verantwortlichen für Organisation, Alarme und Assets.
5.25 Beurteilung und Entscheidung über Informa-tionssicherheitsereignisse	Enginsight unterstützt bei der Bewertung von möglichen Bedrohungen durch die automatisierte Klassifikation dieser vom IDS aufgedeckten Ereignisse. Zum Anderen lassen sich über das SIEM sämtliche durch die Organisation definierten Use-Cases für mögliche Bedrohungen abbilden, um diese automatisiert unternehmensweit aufdecken zu können.
5.26 Reaktion auf Informa-tiossicherheitsvorfälle	Enginsight kann über verschiedene Funktionalitäten Informationen für eine Reaktion und Beurteilung bereitstellen (IDS, SIEM) oder selbst automatisiert reagieren (IPS). Weiterhin bietet Enginsight die Möglichkeit, über die Mikrosegmentierung einen Vorfall einzudämmen. Das SIEM sammelt gleichzeitig unternhemensweit sämtliche Log- und Eventdaten, um diese zu dokumentieren und für spätere forensische Analysen bereitzustellen.
5.28 Sammeln von Beweis-material	Enginsight kann sämtliche protokollierte Daten revisionssicher ablegen. Diese können zu jeder Zeit für forensische Untersuchungen herangezogen werden.
5.29 Informationssicherheit bei Störungen	Bei nicht Erreichbarkeit der Enginsight-Server funktionieren die Agents weiterhin mit den Funktionen (hostbasiertes) IDS und IPS und Mikrosegmentierung.
5.3. Aufgabentrennung	Durch die Vergabe von Rollen und Rechten lassen sich Aufgaben den passenden Verantwortlichen zuweisen.

5.34 Datenschutz und Schutz von personenbezogenen Daten	Die Pseudonymisierung von Daten im SIEM ist frei einstellbar.
5.7. Informationen über die Bedrohungslage	Enginsight unterstützt auf vielfältige Art und Weise beim Erkennen, Protokollieren sowie der Reagieren auf mögliche Bedrohungen. Schwachstellenscans und Pentests generieren ein präventives Bild und identifizieren mögliche Einfallsvektoren. Das Intrusion Detection System (IDS), File Integrity Monitoring (FIM) wie auch das SIEM erkennen mögliche Bedrohungen über die gesamte IT-Infrastruktur hinweg und das Intrusion Prevention System (IPS) bietet die Möglichkeit der automatisierten Reaktion (Bedrohung stoppen).
6. PERSONENBEZOGENE MASSNAHMEN	
6.7 Remote-Arbeit	Durch den auf den Geräten installierten Pulsar-Agent werden diese geschützt, egal in welchem Netzwerk sie sich befinden.
8. TECHNOLOGISCHE MASSNAHMEN	
8.1 Endpunktgeräte des Benutzers	Enginsight unterstützt bei der Endgerätesicherheit durch eine umfassende Protokollierung sämtlicher Events. Dazu zählen auch sämtliche Operationen auf Files (FIM), eine Überwachung der installierten Software und netzwerkseitiger Auffälligkeiten sowie die automatisierte Reaktion und Abschottung des Endpunktgerätes.
8.2 Privilegierte Zugangsrechte	Zugriffe von Benutzern können systemweit wie auch etwa in der O365-Cloud zentral überwacht werden. Über einen entsprechenden SIEM Use-Case können Zugriffe und Zugriffsversuche aufgedeckt und protokolliert werden
8.3 Informationszugangsbeschränkung	Die Mikrosegementierung unterstützt dabei, schnell und unkompliziert die Zugriffe auf kritische Systeme im Netzwerk exakt zu steuern.
8.6 Kapazitätssteruerung	Die Auslastung von Hardware-Ressourcen lässt sich durch Enginsight überwachen (Monitoring).
8.7 Schutz gegen Schadsoftware	Das SIEM unterstützt bei Einbindung von EDR und Enginsight IDS die Identifikation von verdächtigen Netzwerk-Aktivitäten.

8.8 Handhabung von technischen Schwachstellen	Pentest, Observer und Schwachstellenmanagement helfen dabei, technische Schwachstellen und damit einhergehende Bedrohungen frühzeitig und proaktiv zu identifizieren.
8.9 Konfigurationsmanagement	Enginsight überprüft verschiedene Betriebssysteme hinsichtlich ihrer Konfiguration und liefert Empfehlungen, wie die entsprechenden Systeme gehärtet werden können.
8.11 Datenmaskierung	Enginsight bietet die Möglichkeit, sensible Daten, die über das IDS oder auch das SIEM gesammelt werden, zu pseudonymisieren. Die Organisation kann dabei je nach Anforderungen selbst festlegen, welche Daten durch welche Rolle eingesehen werden können.
8.15 Protokollierung	Sämtliche Protokolle, Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse können durch Enginsight SIEM gespeichert, geschützt und analysiert werden. Dabei können verschiedenste Ereignisse und Uscases umgesetzt werden, wie etwa: erfolgreiche und abgelehnte Systemzugriffsversuche; erfolgreiche und abgelehnte Versuche, auf Daten oder andere Ressourcen zuzugreifen; Änderungen der Systemkonfiguration; Nutzung von Privilegien; Nutzung von Dienstprogrammen und Anwendungen; Dateien, auf die zugegriffen wurde, und die Art des Zugriffs, einschließlich des Löschens wichtiger Dateien; vom Zugriffskontrollsystem ausgelöste Alarme; Aktivierung und Deaktivierung von Sicherheitssystemen wie Anti-Virussystemen und IDS; Erstellung, Änderung oder Löschung von Identitäten; Transaktionen, die von Benutzern in Anwendungen ausgeführt werden. In einigen Fällen handelt es sich bei den Anwendungen um einen Dienst oder ein Produkt, das von einem Dritten bereitgestellt oder betrieben wird.
8.16 Überwachung von Aktivitäten	Das Enginsight IDS kann sehr umfassend anormales Verhalten im Netzwerk identifizieren. In Kombination mit dem Enginsight SIEM werden weitere Datenquellen genutzt, um eine umfassendes Bild zu zeichnen. Dabei können folgende Themen mit berücksichtigt werden: ausgehender und eingehender Netzwerk-, System- und Anwendungsverkehr, Protokolle von Sicherheitstools [z. B. Antivirus, IDS, Angriffsabwehrsystem (IPS), Webfilter, Firewalls, Verhinderung von Datenlecks], Ereignisprotokolle zu System- und Netzwerkaktivitäten, Nutzung der Ressourcen (z. B. Prozessor, Festplatten, Speicher, Bandbreite) und deren Leistung. Dabei ist weiterführend auch ein Baselining möglich, um ausgehend von einem "Normalzustand" Abweichungen automatisiert und unterstützt durch Maschine-Learning zu erkennen.

8.19 Installation von Software auf Systemen im Betrieb	Enginsight bietet die Möglichkeit, die installierten Softwarestände aller Server und Clientsysteme zu überwachen. Über Änderungen am Softwarestand können Sie generelle Alarme oder Alarme für spezifische Software konfigurieren.
8.21 Sicherheit von Netzwerkdiensten	Über das Enginsight SIEM können die Event- und Protokolldaten der Netzwerkinfrastruktur und Dienste zentral erfasst und ausgewertet werden.
8.22 Trennung von Netzwerken	Mit Hilfe der Mikrosegmentierung über den Enginsight Pulsar Agent entsteht die Möglichkeit, schnell und effizient kritische Systeme in kleine gekapselte Mikrosegmente zu organisieren.
8.31 Trennung von Entwicklungs-, Test- und Produktionsumgebung	Die Mikrosegmentierung über den Pulsar Agent ermöglicht die schnelle und unkompliziete Trennung von Entwicklungs-, Test- und Produktionsumgebungen.

ENGINSIGHT

ENGINSIGHT GmbH
Leutragraben 1
07743 Jena

+49 3641 271 49-39
hello@enginsight.com
enginsight.com