

ISEC7 CLASSIFY

Keine Klassifizierung, kein Versand.

Nutzer kennzeichnen vertrauliche Dokumente korrekt und geben sie richtig weiter, in jeder Office-Anwendung, auf jedem Gerät. ISEC7 CLASSIFY prüft die Empfänger, bevor eine Nachricht verschickt wird.

Eine Oberfläche
Microsoft Outlook auf dem Desktop und im Web, Android, iOS

BUND, NATO, TLP
fertige Standards, US-Schemata auf Anfrage

Ergänzt Purview
Labels in beide Richtungen synchron

Datensouverän
souveräne Software aus Deutschland von der ISEC7 Group

HERAUSFORDERUNG

Ohne Klassifizierung wird Cybersicherheit zum Blindflug.

Firewall, EDR und SOC sind da. Aber wissen Sie, welche Daten kritisch sind, wer sie erhält und was nie nach außen darf? ISO/IEC 27001:2022 hat dafür zwei eigene Maßnahmen: A.5.12 für die Klassifizierung und A.5.13 für die Kennzeichnung von Informationen. Wer für US-Behörden arbeitet, braucht nach DoD Manual 5200.01, DoD Instruction 5200.48 (CUI) und CMMC geprüfte und durchgesetzte Kennzeichnungen.

CHANCE

Nutzer stufen E-Mails, Anhänge und Office-Dokumente dort ein, wo sie ohnehin arbeiten. Bevor eine Nachricht rausgeht, vergleicht ISEC7 CLASSIFY die Einstufung mit den Empfängeradressen.

- Pflichtfelder: ohne vollständige Kennzeichnung kein Senden und kein Speichern, auch bei Kalendereinträgen und Dokumenten, soweit unterstützt
- Domänen prüfen: Bei vertraulichen Inhalten an fremde Domänen wird blockiert oder gewarnt
- Jeder Anhang einzeln gekennzeichnet
- Jeder Abschnitt einzeln: Betreff, Text oder Absätze, mit Banner, Caveats und Hinweisen
- Netzbewusst: Verfügbare Stufen folgen der Sicherheitsstufe des Netzes

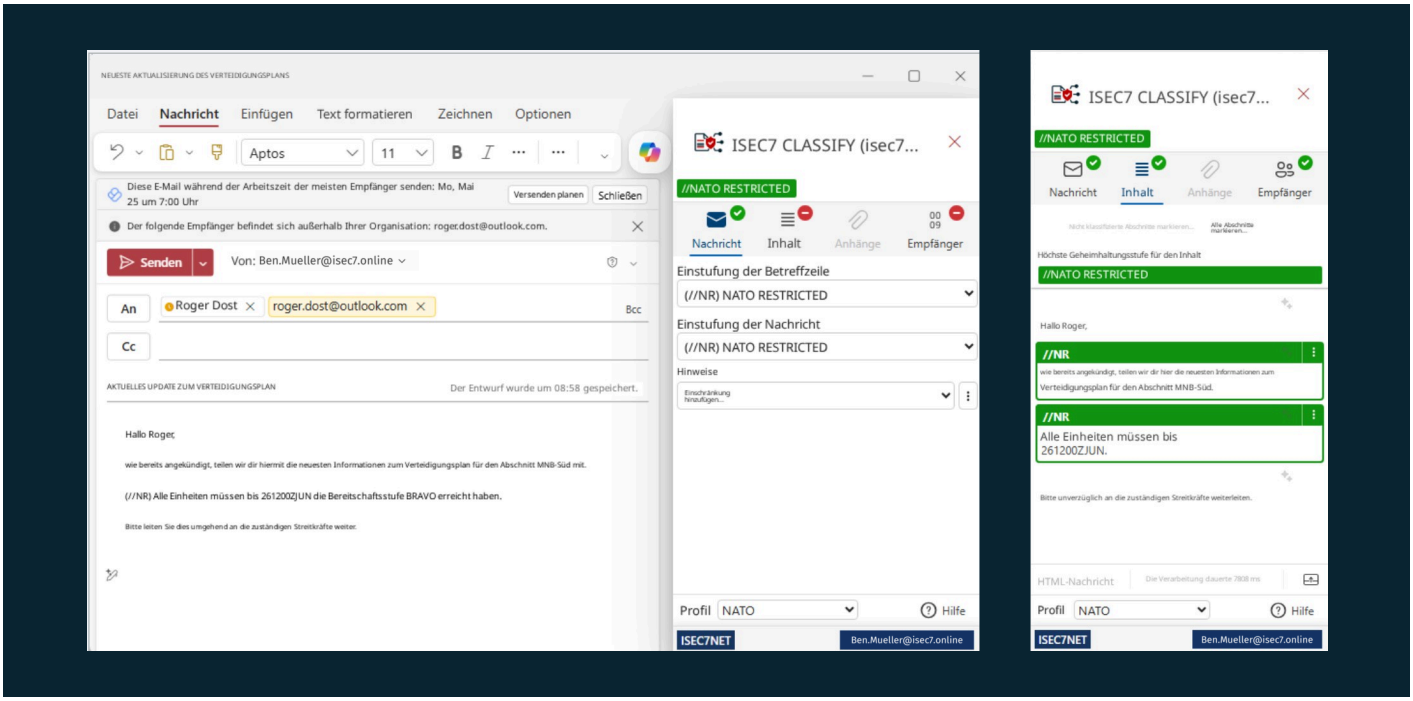
DIE LÖSUNG & USP

- Eine Oberfläche auf allen Clients: Microsoft Outlook, Outlook im Web, Word, Excel, PowerPoint und SharePoint sowie ISEC7 MAIL auf iOS und Android, für Microsoft 365 und On-Premises-Umgebungen
- Mehrere Schemata gleichzeitig: Nutzer wechseln zwischen Profilen
- Multilateral: Klassifizieren über Organisationsgrenzen, zwischen Ländern, Bereichen, AD-Gruppen und einzelnen Nutzern
- Fertige Standards und eigene Schemata: BUND, NATO und TLP sind dabei, US-Schemata (USCLASS, CUI) auf autorisierte Anfrage. Eigene entstehen im Schema-Editor von ISEC7 SPHERE
- Gehostet als Azure Platform as a Service, auf dem Desktop wird nichts installiert
- Revision laufend aktiv: Audit und Statistik in ISEC7 SPHERE, auch für SharePoint und Teams

ZIELGRUPPE

- Behörden und Organisationen mit Sicherheitsanforderungen (NIS2, BOS, KRITIS)
- Öffentliche Verwaltungen, die nach VSA oder mit einem ISMS arbeiten
- Unternehmen, die sensible Informationen in der Lieferkette weitergeben
- Unternehmen mit vertraulichem Know-how oder geistigem Eigentum

Die ISEC7 Group betreibt seit 2003 Digital Workplace und Managed Mobility Services. Für Behörden, internationale Konzerne, KRITIS-Betreiber, geheimschutzbetreute Unternehmen und alle Organisationen, die hohe Compliance-Anforderungen erfüllen müssen. Über 700 Kunden weltweit, darunter Regierungen, Polizeibehörden und Streitkräfte. Der Hauptsitz von ISEC7 ist in Deutschland, weitere Standorte gibt es in den USA, Australien, Neuseeland und Polen.



ISEC7 CLASSIFY UND MICROSOFT PURVIEW

Einmal klassifizieren, überall geschützt.

Vertraulichkeitslabels in Microsoft Purview lösen Verschlüsselung, Markierung und Zugriffsregeln aus. ISEC7 CLASSIFY bringt eine native MIP-Integration mit, Labels sind in beide Richtungen synchron. Und es bietet deutlich mehr: Es läuft auf dem PC, in Microsoft 365 und auf Mobilgeräten und prüft vor dem Versand, ob die Empfänger für die Einstufung berechtigt sind.

ANWENDUNGSBEREICHE

- Word, Excel, PowerPoint: gekennzeichnet Absatz für Absatz, bis zur einzelnen Zelle, jede Folie zeigt ihre Stufe
- SharePoint Online: drei Banner auf drei Ebenen (Tenant, Website, Seite), Kennzeichnung bis in Ordner- und Dateinamen

LOKALE KI

Die KI arbeitet nur lokal, ohne Internet.
Keine Daten verlassen das Gerät.

- Erkennt sensible Inhalte und meldet den Fund, solange keine Kennzeichnung gewählt ist
- Schlägt je Abschnitt eine Kennzeichnung vor, ein Sensitivitätswert zeigt die Relevanz
- Modelle: CUI/NIS2 (Deutsch, Englisch) mit 115 CUI-Unterkategorien für die Kennzeichnung, Security Classification Guide (Englisch) für die Einstufung

US-VORGABEN

- CUI nach 32 CFR 2002 und DoD Instruction 5200.48, mit vorbefülltem CUI Designation Indicator und Authority Block
- DoD Manual 5200.01: Banner-, Abschnitts- und Betreffkennzeichnung, mit Caveats
- CMMC 2.0 und NIST SP 800-171: Audit-Trails in ISEC7 SPHERE liefern Nachweise für die Vorbereitung auf das Assessment. ISEC7 ist kein C3PAO
- DFARS 252.204-7019: unterstützt DoD-Auftragnehmer, die CUI verarbeiten, in Anlehnung an NIST SP 800-171
- DoD Zero Trust: Klassifizierung und Tagging im Data Pillar (Activity 3.2.2), dazu FISMA
- CSfC: erfüllt mit ISEC7 SPHERE die Continuous-Monitoring-Anforderungen des Mobile Access Capability Package
- NIPRNet, SIPRNet und JWICS. Microsoft 365 GCC, GCC High und DoD, FedRAMP Authorized Path

MEHR ERFAHREN

www.isec7.com/de/solutions/isec7-classify

ISEC7
THE DIGITAL WORKPLACE COMPANY
Schellerdamm 16, 21079 Hamburg
isec7.com
sales@isec7.com
+49 40 325076 0