



Herzlich willkommen

Ihre Kommunikation mit M365 nach
innen und außen!

—

Aber sicher!

Inhalt

- 1 Wer bin ich?
- 2 Warum ist sichere Kommunikation wichtig?
- 3 M365 und seine Rolle im Thema sichere Kommunikation
- 4 Best Practices für sichere Kommunikation

Wer bin ich?

Dirk Schönfeld

Head of Consulting | Team Lead ECM



amexus Informationstechnik GmbH & Co. KG
Von-Braun-Str. 34
48683 Ahaus



+49 2561 /9303-727



dschoenfeld@amexus.com



“Stillstand bedeutet
Rückschritt!”



Warum ist sichere Kommunikation
wichtig?

29.02.24

DRK-Kreisverband ist Opfer eines Cy



Wege geleitet, um den Angriff einz

sensibler Daten zu gewährleisten. ,

der von uns gespeicherten Daten f

und wir versichern Ihnen, dass alle

ergriffen werden, um die Situation

Kreisgeschäftsführerin Christiane S

Dazu wurden alle Systeme vorerst

telefonische Erreichbarkeit bzw. die

Mail aktuell eingeschränkt ist. Wich

112 und der Hausnotruf von diese

weiterhin uneingeschränkt funktion

Das Spezialisten-Team arbeitet auf

wiederherzustellen. Jedoch kann es

Verzögerungen im E-Mail-Verkehr und bei Zahlungsv

kommen. Für mögliche Unannehmlichkeiten bittet der

Verständnis

 2. Februar 2024

Cyberangriff auf Krankenhäuser in Nordrhein-Westfalen, Deutschland

Dreifaltigkeits-Hospital - Lippstadt, Nordrhein-Westfalen, Deutschland (Kreis Soest)

Betroffen sind ebenfalls: Marien-Hospital Erwitte, Hospital zum Heiligen Geist Geseke

[Wieder Hacker-Angriff im Kreis Soest: Keine OP und Neuaufnahmen in drei](#)

Wichtige Updates zum Datenschutzvorfall

14. März 2024

Sehr geehrte Geschäftspartner und Interessenten,

Wir müssen leider gesichert davon ausgehen, dass abgezogene Daten im Internet (Darknet) zur Verfügung gestellt wurden.

Wir arbeiten weiterhin eng mit den Strafverfolgungsbehörden zusammen, um den Vorfall aufzuklären. Wir nehmen diese Situation sehr ernst und behandeln sie mit höchster Priorität.

Auch weiterhin gilt: Falls Sie ungewöhnliche Aktivitäten oder verdächtige Vorfälle bemerken, bitten wir Sie dringend, dies entweder der örtlichen Polizei oder unserem Krisenmanagement-Team zu melden.

Wir danken Ihnen herzlich für Ihr Verständnis und Ihre fortlaufende Unterstützung.

Mit freundlichen Grüßen

Hackergruppe Lockbit veröffentlicht von der Deutschen Energie-Agentur (dena) gestohlene Daten im Darknet.

t
" sind laut einem
ten online zu
gestohlen -

Gründe für sichere Kommunikation



Schutz sensibler
Informationen



Compliance und
Datenschutz



Verhinderung von
Datenverlust



Vertrauen und
Reputation



Cybersicherheit und
Bedrohung



Effizienz und
Produktivität

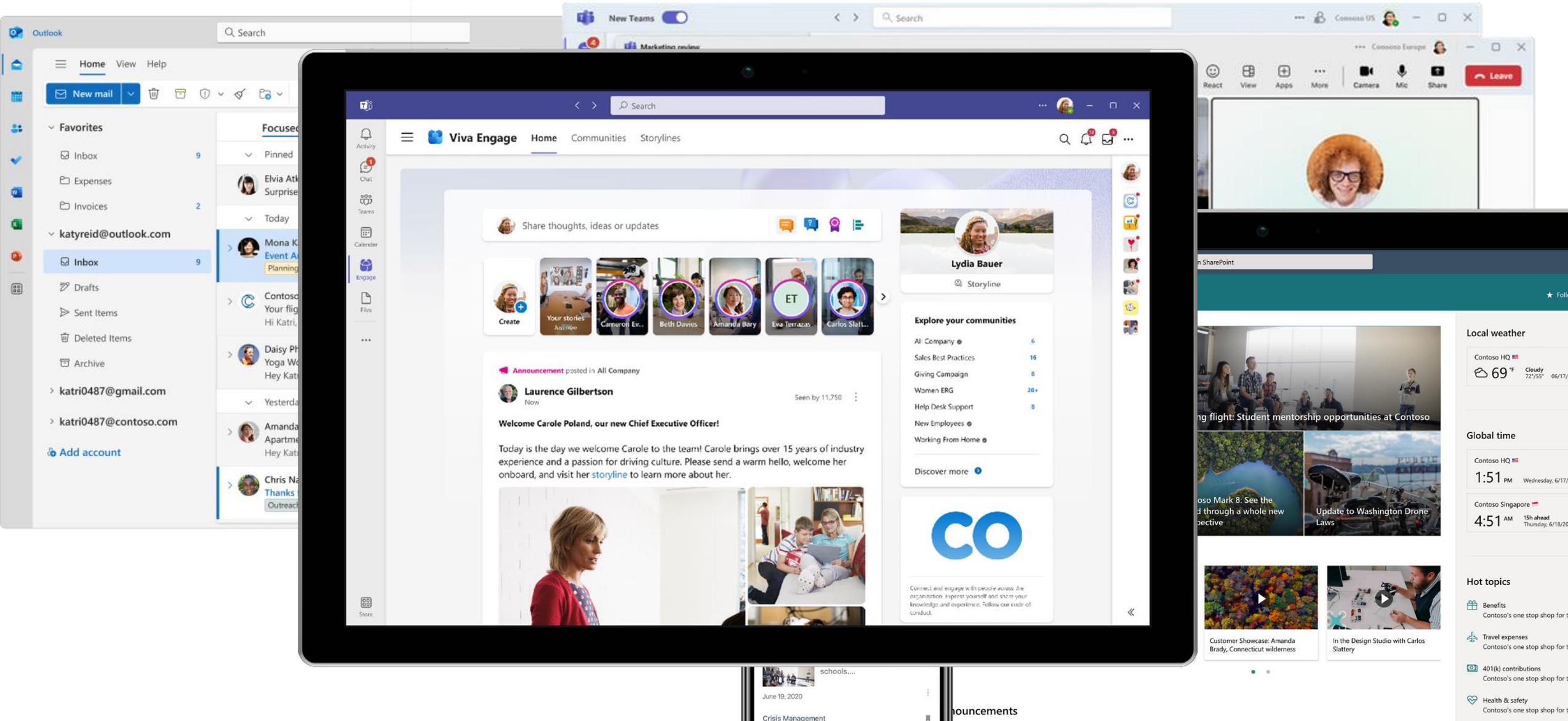
Gewährleistung der Integrität,
Vertraulichkeit und Verfügbarkeit von
Informationen

Schutz der Organisation vor potenziellen
Risiken



M365 und seine Rolle im Thema sichere Kommunikation

Tools und Plattformen für Kommunikation in M365



Möglichkeiten zur sicheren Gestaltung der Kommunikation



Multi-Faktor-
Authentifizierung
(MFA)



Verwaltung mobiler
Geräte



Verschlüsselung



Berechtigungs-
management



Datenklassifizierung



Sicherheitsbewusstsein
schärfen

Sichere Gestaltung des Dateimanagements



Data Loss Prevention (DLP) –
Richtlinien



Zusammenarbeit mit Gästen
und externer Zugriff



Sensitivity Labels



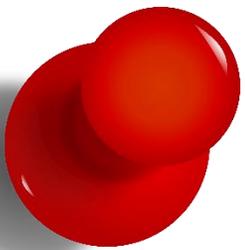
Information Rights
Management (IRM)

LIVE



Best Practices für sichere Kommunikation





Finden Sie die richtige Lizenzierung

Microsoft 365

E3

Grundlegende Sicherheitsfunktionen sind in dieser Lizenz enthalten

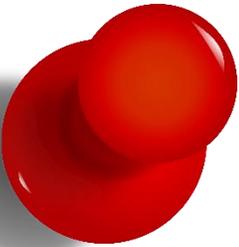
- **Azure Information Protection**
- **Microsoft Defender for Business**
- **Azure Active Directory Premium P1** für Identitäts- und Zugriffsverwaltung

Microsoft 365

E5

Erweiterte Sicherheits- und Compliance-Funktionen im Vergleich zu E3

- **Microsoft Defender XDR:** Integrierter Schutz gegen schädliche Angriffe.
- **Advanced Threat Analytics:** Erkennt und untersucht Bedrohungen auf Endpunkten.
- **Azure Information Protection P2:** Erweiterte Funktionen für Datenklassifizierung und Verschlüsselung.
- **Compliance Manager:** Vereinfacht die Compliance-Bewertung.
- **Insider Risk Management:** Identifiziert riskante Aktivitäten in der Organisation
- **Microsoft Purview:** Datengovernance, Risiko und Compliance in einer integrierten Lösung.
- **Message Encryption:** Verschlüsselte E-Mail-Kommunikation.
- **Privileged Access Management:** Kontrolle über privilegierte Admin-Aufgaben.



Schulung der Mitarbeitenden

Regelmäßige Schulungen

- Sensibilisieren Sie Ihre Mitarbeiter für die Risiken von unsicherer Kommunikation, Phishing-Angriffe und Social Engineering.
- Zeigen Sie praktische Anwendungsfälle für sichere Kommunikation in M365

Integration in den Arbeitsalltag

- Integrieren Sie Sicherheitsschulungen in den täglichen Arbeitsablauf.
- Zeigen Sie, wie Sicherheitsrichtlinien in der Praxis angewendet werden.

Schulungen durch Experten und Bereitstellung von Ressourcen

- Bieten Sie Schulungen durch Branchenexperten an, um spezifische Szenarien und Best Practices zu vermitteln.
- Stellen Sie Handbücher, Leitfäden und Videos zur Verfügung und ermutigen Sie diese zu nutzen.



Schaffen von Regelwerken

Governance Framework für die Zusammenarbeit

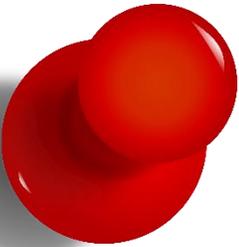
- Berechtigungsmodelle und Zugriffssteuerung
- Datenklassifizierung und Datenschutz
- Überwachung und Compliance

Teamsnutzungskonzept

- Themen für die IT-Administration
- Themen für die Mitarbeitenden
- Adoption und Betreuung

Kommunikationskonzept

- Kommunikationskanäle – Wann soll welches Tool genutzt werden?
- Zielgruppen – Welche Zielgruppen für Kommunikation gibt es?



Security Score Bewertung beachten

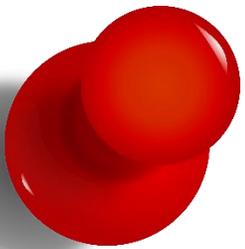
Der Secure Score misst den Sicherheitsstatus einer Organisation und zeigt an, wie viele empfohlene Maßnahmen bereits umgesetzt wurden

Wie funktioniert der Score?

- Es gibt Punkte für verschiedene Aktionen
 - Konfiguration empfohlener Sicherheitsfunktionen
 - Durchführung sicherheitsrelevanter Aufgaben
 - Umsetzung von Empfehlungen durch Drittanbieterlösungen

Balance zwischen Sicherheit und Usability

- Beachten Sie, dass nicht jede Empfehlung für Ihre Umgebung geeignet ist
- Sicherheit sollte immer im Einklang mit der Benutzerfreundlichkeit stehen



Security Score Bewertung beachten

Microsoft Defender
Suchen

- Start
- Vorfälle & Warnungen
- Aktionen und Übermittlung...
- Informationen über Bedroh...
- Sicherheitsbewertung**
- Testversionen
- E-Mail & Zusammenarbeit
- Untersuchungen
- Explorer
- Überprüfen
- Kampagnen
- Bedrohungs-Tracker
- Exchange-Nachrichtenablaufver...
- Richtlinien und Regeln
- Berichte
- Überwachen
- Status
- Berechtigungen
- Einstellungen
- Weitere Ressourcen
- Navigation anpassen

Microsoft-Sicherheitsbewertung

Loading...

Übersicht Empfohlene Maßnahmen Verlauf Metriken und Trends

Microsoft-Sicherheitsbewertung ist eine Darstellung des Sicherheitsstatus Ihrer Organisation und ihrer Möglichkeiten, ihn zu verbessern.

Angewendete Filter: Filter

Ihre Sicherheitsbewertung

Sicherheitsbewertung: 84...

54/64 erzielte Punkte

Punkte aufgliedern nach: **Kategorie**

- Identität: **91,07%**
- Apps: **87,5%**

■ Erzielte Punkte ■ Chance

Zu prüfende Aktionen

Verschlechtert	Zu behandeln	Geplant	Risiko akzeptiert	Zuletzt hinzugefügt
0	5	0	0	0
Kürzlich aktualisiert				
0				

Am häufigsten empfohlene Aktionen

Empfohlene Maßnahme	Bewertung...	Status	Kategorie
Stellen Sie sicher, dass die Benutzer zustimmen, dass Apps, ni...	+6.25 %	<input type="radio"/> Zu behandeln	Identität
Nur eingeladene Benutzer sollten automatisch zu Microsoft T...	+3.13 %	<input type="radio"/> Zu behandeln	Apps
Konfigurieren, welche Benutzer in Microsoft Teams-Besprech...	+3.13 %	<input type="radio"/> Zu behandeln	Apps
Anonymen Benutzern die Teilnahme an Besprechungen einsc...	+1.56 %	<input type="radio"/> Zu behandeln	Apps
Administratorrollen mit den geringsten Berechtigungen verw...	+1.56 %	<input type="radio"/> Zu behandeln	Identität
Stellen Sie sicher, dass die mehrstufige Authentifizierung für ...	+15.63 %	<input checked="" type="radio"/> Abgeschlossen	Identität
Stellen Sie sicher, dass die mehrstufige Authentifizierung für ...	+14.06 %	<input checked="" type="radio"/> Abgeschlossen	Identität
Aktivieren von Richtlinien für bedingten Zugriff zum Blockier...	+12.5 %	<input checked="" type="radio"/> Abgeschlossen	Identität

[Alle anzeigen](#)

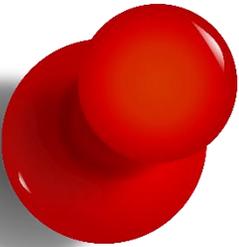
Vergleich

Ihre Bewertung	84.38 / 100.01
Organisationen ähnlicher Größe	46.73 / 100

Verlauf

Ressourcen

Nachrichten von Microsoft



Mitnahme des Datenschutzbeauftragten

Informieren und sensibilisieren

- Stellen Sie sicher, dass der Datenschutzbeauftragte vom ersten Moment an dabei ist
- Erklären Sie die Ziele, den Umfang und die Sicherheitsaspekte der Kommunikation mit M365

Beteiligung bei der Erstellung von Richtlinien und Konzepten

- Der Datenschutzbeauftragte sollte in die Erstellung von Kommunikationsrichtlinien und -konzepten einbezogen werden
- Berücksichtigen Sie Datenschutzaspekte und Compliance-Anforderungen

Regelmäßige Abstimmung und Zusammenarbeit

- Halten Sie regelmäßige Abstimmungen mit dem Datenschutzbeauftragten ab
- Gemeinsam können Sie sicherstellen, dass Datenschutzrichtlinien eingehalten werden



Danke

Pause