

## Sicherheitsmaßnahmen für den ERP-Betrieb

### Kurzbeitrag

Dennis Buckenauer<sup>1</sup> und Sandy Eggert<sup>2</sup>

**Abstract:** In dieser Forschungsarbeit wurden zunächst allgemeine IT-Sicherheitsbedrohungen im Bereich kleiner und mittlerer Unternehmen betrachtet. Anschließend erfolgte die Identifikation von Sicherheitslücken im IT-Betrieb, mit dem Fokus auf der Nutzung von ERP-Systemen. Eine Umfrage zu Sicherheitsrisiken und Schutzmaßnahmen untermauerte die Notwendigkeit für Unternehmen, einen proaktiven und ganzheitlichen Ansatz zur Gewährleistung der Sicherheit im ERP-Betrieb zu verfolgen. Die Identifikation von Schwachstellen und die Implementierung von Schutzmaßnahmen sind entscheidend, um die Sicherheit und Integrität von Unternehmensdaten zu gewährleisten. Die Ergebnisse der Arbeit mündeten in die Entwicklung eines Sicherheitsleitfadens, welcher speziell auf die Sicherheit des Einsatzes von ERP-Systemen in kleinen und mittleren Unternehmen abzielt.

**Keywords:** Sicherheitsrisiken, Sicherheitslücken, Schutzmaßnahmen, Sicherheitsleitfaden, ERP-Betrieb.

## 1 Einleitung

Kleine und mittlere Unternehmen sind heutzutage einer Vielzahl von IT-Sicherheitsbedrohungen ausgesetzt [BJ18]. Dies zeigt u.a. eine Untersuchung der Bitkom, in der die Arten digitaler IT-Angriffe erhoben wurden, die in Unternehmen entsprechende Schäden verursacht haben [Bi23]. Am häufigsten wurden Phishing-Angriffe mit 31% genannt, gefolgt von Angriffen auf Passwörter (29%) und Infektionen mit Schadsoftware bzw. Malware (28%). Ransomware-Angriffe (23%) sind nach wie vor ein großes Problem, da sie zu erheblichen Datenverlusten und finanziellen Schäden führen können. SQL-Injection-Angriffe (21%) stellen ein Risiko für die Datensicherheit dar, während Spoofing-Angriffe (14%) und DDoS-Attacken (12%) Betriebsunterbrechungen verursachen können. Weniger häufig, aber dennoch ernstzunehmende Bedrohungen sind Cross-Site-Scripting (XSS) (10%), Man-in-the-Middle-Angriffe (7%) und CEO Fraud (6%) [Bi23]. Diese hohen Angriffszahlen deuten drauf hin, dass das Bewusstsein für die Notwendigkeit einer systematischen Herangehensweise an die Informationssicherheit noch nicht ausreichend verbreitet ist und Sicherheitsmaßnahmen in Unternehmen unzureichend implementiert sind. Ziel ist es, Maßnahmen zu identifizieren, die die Sicherheit im IT-Betrieb von KMU erhöhen. Da mehr als die Hälfte der deutschen KMU ein ERP-System nutzen [Bi23], liegt der Fokus der Betrachtung auf den ERP-Betrieb.

---

<sup>1</sup> HWR Berlin, Badensche Str. 52, 10825 Berlin, dennis.buckenauer@gmail.com,

<sup>2</sup> HWR Berlin, Badensche Str. 52, 10825 Berlin, sandy.eggert@hwr-berlin.de

## 2 Identifikation von Sicherheitslücken

Um technische und organisatorische Schutzmaßnahmen ableiten zu können, erfolgte zunächst die Identifikation und Einordnung von Sicherheitslücken. Dazu wurde neben einer Literaturuntersuchung eine Onlinebefragung von Unternehmen aus dem Bereich KMU im Zeitraum von Januar bis Februar 2024 herangezogen. Die Befragung fand im Rahmen einer ERP-Marktstudie [Eg24] statt, an der sich insgesamt 64 ERP-Anbieter- und -Dienstleistungsunternehmen beteiligt haben. Folgende Fragen wurden im Bereich der IT-Sicherheit beantwortet:

- Was waren aus Ihrer Sicht die häufigsten Sicherheitsrisiken im Jahr 2023?
- Welche Schutzmaßnahmen setzen Sie für Ihr ERP-System ein?

Abbildung 1 (links) zeigt die prozentuale Verteilung verschiedener Angriffsarten. Die Ergebnisse zeigen, dass Phishing-E-Mails mit 53% den häufigsten Angriffstyp darstellen, gefolgt von Credential Sniffing (13%) und Cross-Site Scripting (13%). Diese Ergebnisse betonen die fortwährende Relevanz von Phishing als eine der vorherrschenden Bedrohungen im Bereich der IT-Sicherheit. Des Weiteren wird ersichtlich, dass DDoS-Angriffe mit 9% der gemeldeten Vorfälle signifikant vertreten sind, was auf die kontinuierliche Bedrohung durch Verfügbarkeitsangriffe hinweist. Ebenso sind Angriffe wie SQL-Injection (8%) und Man-in-the-Middle (5%) relevante Bedrohungen, die auf Schwachstellen in der Software und Netzwerkinfrastruktur abzielen. Die Präsenz von physischen Angriffen (11%) weist daraufhin, dass die Sicherheit der physischen Infrastruktur von Unternehmen ebenso wichtig ist, wie die Sicherheit der digitalen Systeme.

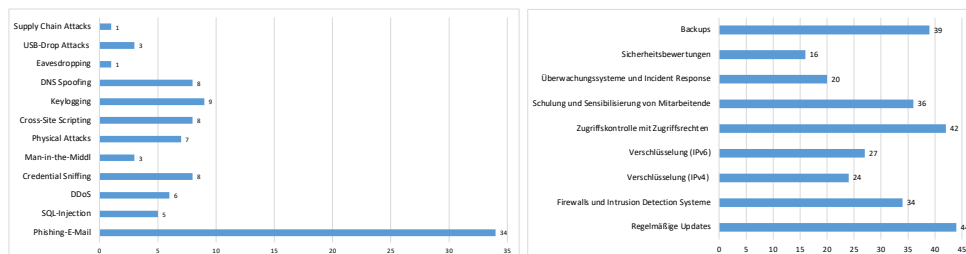


Abb. 1: Häufigkeit von Sicherheitsrisiken nach Angriffsarten (links) und Implementierungen von Sicherheitsmaßnahmen (rechts), n=64

Eine Übersicht, welche Sicherheitsmaßnahmen ERP-Anbieter und -Dienstleister bereits in ihren Systemen implementiert haben, zeigt die Abbildung 1 (rechts). Aus den Daten geht hervor, dass mehr als 60 % der befragten Unternehmen „regelmäßige Updates“, „Zugangskontrolle mit Zugriffsrechten“ und „Backups“ systemseitig implementiert haben. Deutlich mehr als die Hälfte der Unternehmen gaben an „Schulung und Sensibilisierung der Mitarbeiter“ in ihren Projekten einzugliedern. Weiterhin werden Firewalls und Intrusion Detection Systeme von etwas mehr als der Hälfte der Systemanbieter implementiert.

### 3 Schutzmaßnahmen

Im Rahmen der Literaturstudie wurden unterschiedliche Schutzmaßnahmen identifiziert und in technische und organisatorische Maßnahmen gegliedert.

#### 3.1 Technische Schutzmaßnahmen

Die Sicherung von Unternehmensdaten in ERP-Systemen stellt insbesondere für kleine und mittlere Unternehmen aufgrund der damit einhergehenden Kosten und Personaleinsatzes eine große Herausforderung dar. Effektive Sicherheit in ERP-Systemen erfordert eine Kombination verschiedener technischer Schutzmaßnahmen, die speziell darauf ausgelegt sind, die Integrität, Vertraulichkeit und Verfügbarkeit sensibler Informationen zu gewährleisten. Folgende Schutzmaßnahmen wurden identifiziert:

**Firewall- und Virenschutzsysteme:** Die Kombination von Firewall- und Virenschutzsystemen bildet eine grundlegende Verteidigungslinie für ERP-Systeme in KMU. Durch die Implementierung von Richtlinien und regelmäßigen Updates können sie dazu beitragen, das Risiko von Angriffen zu minimieren und die Integrität der Unternehmensdaten zu schützen [Bu21].

**Verschlüsselungstechnologien:** Grundsätzlich sind im Rahmen der Verschlüsselungstechnologien in der Informationssicherheit die symmetrische und die asymmetrische Verschlüsselung zu unterscheiden. Hinzu kommen hybride Verschlüsselungsverfahren, die eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung verwenden. Diese kombinierten Methoden bieten eine ausgewogene Lösung zwischen Sicherheit und Effizienz und werden oft in komplexen Sicherheitsumgebungen eingesetzt. Ein effektives Schlüsselmanagement ist entscheidend, um die Sicherheit der verschlüsselten Daten zu gewährleisten [BS24].

**System- und Netzwerküberwachung:** Die Überwachung von ERP-Systemen und Netzwerken ermöglicht die frühzeitige Identifikation von Sicherheitsvorfällen. Überwachungssysteme bieten Einblicke in Geräte und Verbindungen und unterstützen IT-Experten bei der Identifizierung und Meldung von Fehlern, der Planung von Wartungsmaßnahmen und der Einhaltung von Compliance- und Sicherheitsstandards. Sie tragen dazu bei, Netzausfälle zu vermeiden und die Ressourcen für IT-Anpassungen zu optimieren [Sh23]. Identifizierte Faktoren im Rahmen der System- und Netzwerküberwachung sind: Früherkennung von Sicherheitsvorfällen, Tools und Methoden für die Überwachung sowie Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS). IDS und IPS bieten eine eingehende Überprüfung und Identifikation potenzieller Sicherheitsbedrohungen im Vergleich zu herkömmlichen Firewalls und Virenschutzsystemen und sind in der Lage, sowohl bekannte als auch unbekannte Bedrohungen zu identifizieren und genauere Informationen über die Art und Herkunft des Angriffs bereitzustellen. Durch die Echtzeitüberwachung des Netzwerkverkehrs können sie auf verdächtige Aktivitäten reagieren und potenzielle Angriffe abwehren [Ma23].

### 3.2 Organisatorische Sicherheitsmaßnahmen

**Schulungen und Sensibilisierung:** Schulungen und Sensibilisierungsmaßnahmen spielen eine maßgebliche Rolle, um die Mitarbeitenden für Sicherheitsrisiken zu sensibilisieren und bewusstes Verhalten zu fördern [Is23].

**Erstellung von Sicherheitsrichtlinien:** Sicherheitsrichtlinien dienen als Regeln, die konfiguriert werden können, um Ressourcen auf einem Gerät oder Netzwerk zu schützen. Sie sollten als integraler Bestandteil der allgemeinen Sicherheitsimplementierung verwendet werden, um Domänencontroller, Server, Clientgeräte und andere Ressourcen in einer Organisation zu schützen [CY24].

**Incident Response Plan:** Die Entwicklung und Implementierung eines Incident Response Plans (IRP) für ERP-Systeme ist ein entscheidender Schritt, um auf Sicherheitsvorfälle schnell und effektiv reagieren zu können. ERP-Systeme sind zentrale Komponenten der IT-Infrastruktur in Unternehmen, verarbeiten sensible Daten und stellen dadurch ein attraktives Ziel für Sicherheitsangriffe dar [BS21].

## 4 Erste Ergebnisse und Ausblick

Im ersten Schritt wurde ein Sicherheitsleitfaden konzipiert, der KMU dabei unterstützt, systematisch sicherheitsrelevante Aspekte zu überprüfen und geeignete Maßnahmen zu ergreifen und aktuelle Lücken im Sicherheitsmanagement zu identifizieren.

	erfüllt	teilweise umsetzung	umsetzung in der weg	nicht erfüllt
<b>1. Entwicklung von Sicherheitsrichtlinien:</b>				
Festlegung klarer Anforderungen an das Passwortmanagement				
Verbot der Installation von nicht autorisierter Software				
Beschränkung der Nutzung von externen Speichermedien				
<b>2. Benutzerschulung und Sensibilisierung:</b>				
Schulung der Mitarbeitenden zur sicheren Nutzung von ERP-Systemen und den Umgang mit sensiblen Daten.				
Sensibilisierung für Phishing-Angriffe und andere Cyber-Bedrohungen sowie Maßnahmen zur Erkennung und Vermeidung.				
Integration von regelmäßigen Schulungen und Schulungsmaterialien in die Onboarding-Prozesse neuer Mitarbeitenden.				
Durchführung regelmäßiger Phishing-Tests, um die Reaktionsfähigkeit der Mitarbeitenden zu verbessern.				
<b>3. Zugriffskontrolle:</b>				
Ermittlung und Dokumentation aller Benutzernden, die Zugriff auf das ERP-System haben.				
Implementierung von strengen Zugriffskontrollen und Berechtigungsstufen basierend auf den Rollen und Verantwortlichkeiten der Benutzernden.				
Regelmäßige Überprüfung und Aktualisierung von Benutzerberechtigungen.				
Implementierung einer Zwei-Faktor-Authentifizierung zur weiteren Sicherung der Zugriffskontrollen.				
<b>4. Systemintegrität:</b>				
Regelmäßige Überprüfung der Systemintegrität durch Sicherheits- und Penetrationstests.				
Implementierung von Sicherheitspatches und -aktualisierungen für das ERP-System und alle verbundenen Softwarekomponenten.				
Überwachung und Erkennung von Anomalien im Systemverhalten.				
Implementierung eines Systems zur Überwachung von Sicherheitsupdates und Patches.				
<b>5. Compliance und Datenschutz:</b>				
Einhaltung geltender Datenschutzgesetze und -vorschriften, insbesondere im Hinblick auf den Umgang mit personenbezogenen Daten.				
Regelmäßige Überprüfung der Compliance mit branchenspezifischen Standards und Best Practices im Bereich der Informationssicherheit.				
Dokumentation über die Einhaltung von Datenschutzgesetzen.				
Implementierung regelmäßiger interner Überprüfungen und Audits zur Sicherstellung der Einhaltung von Standards und Best Practices.				
<b>6. Datensicherheit:</b>				
Implementierung von Verschlüsselungstechnologien für sensible Daten sowohl während der Speicherung als auch der Übertragung.				
Regelmäßige Sicherung und Archivierung von Daten, einschließlich Offsite-Backups, um im Falle von Datenverlusten wiederherstellen zu können.				
Überwachung und Schutz vor Datenverlust oder -diebstahl durch Zugriffskontrollen und Firewalls.				
Regelmäßige Überprüfung der Effektivität der implementierten Verschlüsselungstechnologien.				
<b>7. Notfallvorsorge und Incident Management:</b>				
Entwicklung eines Notfallplans für den Umgang mit Systemausfällen, Datenverlust oder Sicherheitsverletzungen.				
Einrichtung eines Incident-Response-Teams zur schnellen Reaktion auf Sicherheitsvorfälle.				
Regelmäßige Überprüfung und Aktualisierung des Notfallplans basierend auf aktuellen Bedrohungen und Risiken.				
Durchführung von Simulationen von Sicherheitsvorfällen zur Überprüfung der Wirksamkeit des Notfallplans.				
<b>8. Externe Überwachung und Auditierung:</b>				
Analyse der Ergebnisse externer Audits und Implementierung von Maßnahmen zur Verbesserung der Sicherheit.				
Einbindung externer Sicherheitsexperten in regelmäßige Sicherheitsüberprüfungen und Audits zur unabhängigen Bewertung der Sicherheitsmaßnahmen.				

Abb. 2: Sicherheitsleitfaden für KMU

Durch die Kombination von technischen und organisatorischen Ansätzen verfolgt der Leitfaden einen ganzheitlichen Sicherheitsansatz. Der Leitfaden ermöglicht es den Unternehmen, ihre Sicherheitsmaßnahmen kontinuierlich zu verbessern und sich den sich ständig verändernden Bedrohungslandschaften anzupassen.

In einer weiteren Entwicklungsstufe soll der Leitfaden um einen Maßnahmenkatalog ergänzt werden, der technischen und organisatorische Schutzmaßnahmen mit konkreten Umsetzungsvorschlägen ausstattet.

## Literaturverzeichnis

- [Bi23] Bitkom; Statista: Welche der folgenden Arten von digitalen IT-Angriffen haben innerhalb der letzten 12 Monate in Ihrem Unternehmen einen Schaden verursacht?, <https://de-statista-com.ezproxy.hwr-berlin.de/statistik/daten/studie/928943/umfrage/von--digitalen-angriffen-betroffene-unternehmen-nach-art-des-angriffs/>, Stand: 13.03.2024.
- [BJ18] Bollhöfer, E.; Jäger, A.: Wirtschaftsspionage und Konkurrenzausspähung. Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung, Max-Planck-Institut für ausländisches und internationales Strafrecht eV., Freiburg i.Br., 2018.
- [BS21] BSI, Bundesamt für Sicherheit in der Informationstechnik, APP.4.2: SAP-ERP-System. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium\\_Einzel\\_PDFs\\_2021/06\\_APP\\_Anwendungen/APP\\_4\\_2\\_SAP\\_ERP\\_System\\_Edition\\_2021.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/06_APP_Anwendungen/APP_4_2_SAP_ERP_System_Edition_2021.html), Stand: 03.03.2024.
- [BS24] BSI, Bundesamt für Sicherheit in der Informationstechnik, Arten der Verschlüsselung. <https://www.bsi.bund.de/dok/6597616>, Stand: 06.03.2024.
- [Bu21] van der Burgt, R., 2021. Antiviren-Software vs. Firewall: Was ist der Unterschied? <https://vpnoverview.com/de/antiviren-information/unterschied-antivirus-firewall/>, Stand: 06.02.2024.
- [CY24] Cyberpilot, Kostenlose Vorlage für IT-Sicherheitsrichtlinie – Eine Schritt-für-Schritt-Anleitung. <https://www.cyberpilot.io/de/cyberpilot-blog/it-sicherheitsrichtlinie-eine-schritt-fuer-schritt-anleitung>, Stand: 06.02.2024.
- [Eg24] Eggert, S.: ERP-Marktanalyse 2024. In: ERP Information 1/2024, S. 74-102, DPI Verlag Berlin, 2024.
- [Is23] Isler, K., 2023. Sicherheitsbewusstsein schaffen: Wie Unternehmen ihre Mitarbeiter mit Trainings sensibilisieren können. <https://www.hagel-it.de/it-insights/sicherheitsbewusstsein-schaffen-wie-unternehmen-ihre-mitarbeiter-mit-trainings-sensibilisieren-koennen.html>, Stand: 06.02.2024.
- [Ma23] Mahmood, S., 2023. Der Unterschied zwischen Firewall und IDS, IPS: Die Grundlagen verstehen. <https://nextdoorsec.com/de/der-unterschied-zwischen-firewall-und-ids-ips-die-grundlagen-verstehen/>, Stand: 06.02.2024.
- [Sh23] Sharif, A., 2023. Was ist Netzwerküberwachung? <https://www.crowdstrike.de/cyber-security-101/observability/network-monitoring/>, Stand: 06.02.24.