
# Hacker-Angriffe auf ERP-Systeme:

# Ansätze zum Umgang mit Cyber Security Risiken

Unabhängig davon, ob Unternehmen ihre ERP-Systeme in der Cloud oder lokal betreiben: hundertprozentige Sicherheit gibt es nicht. Mit verschiedenen Stellschrauben lässt sich das Risiko von Angriffen jedoch minimieren.
86 Prozent der Unternehmen in Deutschland haben nach Untersuchungen des Bitkom zuletzt Schäden durch Cyberangriffe davongetragen. Tendenz steigend: Nach Angaben des Branchenverbandes sind die Beeinträchtigungen durch Erpressung, IT-Ausfälle oder die Störung von Betriebsabläufen seit 2019 um 358 Prozent gestiegen.
Trotz dieser Bedrohungslage scheinen viele ERP-Anbieter und -Anwender das Thema Sicherheit jedoch (noch) auf die leichte Schulter zu nehmen: In der Studie „Cloud-ERP 2021" der IDG Research gaben 20 Prozent der befragten Unternehmen an, Cloud-ERP-Security sei ihnen nicht oder überhaupt nicht wichtig. Vielleicht stammt dieses Denken noch aus der Zeit, als die meisten Unternehmen ihre ERP-Systeme lokal auf dem eigenen Server betrieben haben. Aber die ERP-Welt hat sich verändert: Heute wandern immer mehr Anwendungen in die Cloud. Sie sind damit von außen erreichbar und bieten so auch eine größere Angriffsfläche für Hacker.
Auf der anderen Seite verfügen gerade etablierte Cloud-Anbieter wie Amazon Web Services (AWS) oder Microsoft Azure über einen sehr hohen Sicherheitsstandard, der gerade für ein mittelständisches Unternehmen mit einer On-Premises-Lösung nur schwer zu erreichen ist.

## Herausforderung Multicloud

Bezogen auf die Sicherheit spielt es daher gar keine so große Rolle, ob Unternehmen ihre ERP-Systeme lokal oder in der Cloud betreiben. Entscheidend ist vielmehr die Komplexität der gesamten Anwendungslandschaft. Denn die meisten Unternehmen kombinieren ihre ERP-Systeme mit Anwendungen spezialisierter Anbieter aus verschiedenen Clouds, die über Schnittstellen miteinander verbunden sind. Tendenz steigend: Nach Angaben des amerikanischen Cyber Security-Anbieters Vectra AI buchen weltweit inzwischen fast zwei Drittel aller Unternehmen im Wochenrhythmus neue AWS-Dienste. Diese zunehmende und sich kontinuierlich verändernde Vernetzung unterschiedlicher Anwendungen und Systeme birgt jedoch die Gefahr von Lücken und Fehlern, die sich im schlimmsten Fall leider auch Hacker zunutze machen.

> Nach der IDG-Studie „Cloud Security 2021" vermelden in der DACH-Region 39 Prozent der Unternehmen mit 500 bis 999 Beschäftigten in den letzten zwölf Monaten wirtschaftliche Schäden durch Attacken auf die von ihnen genutzten Cloud-Dienste. Bei Unternehmen mit weniger als 500 oder mindestens 1.000 Beschäftigten sind es immer noch 32 Prozent.

Auch die starke Verbreitung agiler Methoden und Continuous Delivery (CD) bei der Anpassung und Entwicklung von (ERP-)Systemen bergen Sicherheitsrisiken. Immer kürzere Zyklen und Release-Zeiten verknappen die Zeit für hinreichende Tests und Erfahrungen im Feld. Das kann nicht nur für die Hersteller zum Problem werden, sondern auch für die Anwenderunternehmen. Denn diese müssen oft in sehr engen Zeitfenstern dafür sorgen, dass die Updates im gesamten Multi-Cloud-Gebilde störungsfrei und sicher funktionieren. Nicht zu vergessen sind zudem mögliche Sicherheitslücken in Open-Source-Bibliotheken (z.B. log4j), die heute auch in sehr vielen kommerziellen Softwarelösungen eingesetzt werden.

**Log4shell**

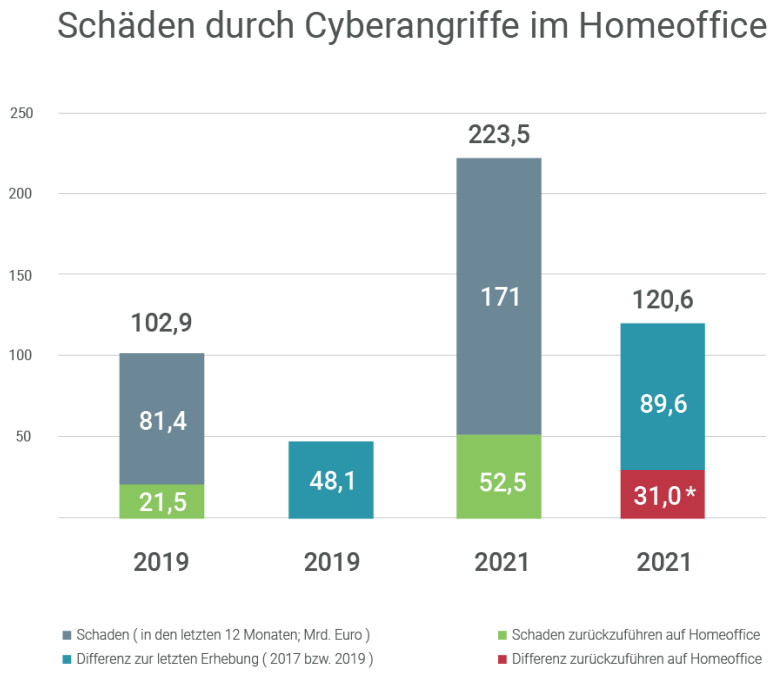
Mitte Dezember schüttelte die Java-Sicherheitslücke "Log4Shell" Deutschlands IT-Abteilungen durch und rückte schlagartig auch bei ERP-Anwendern das Thema Sicherheit in den Fokus. Die Schwachstelle, die in der weit verbreiteten Log4j Protokollierungsbibliothek für Java-Anwendungen auftauchte, gilt als größte Sicherheitslücke in der Geschichte des Internets. Das Problem: Log4shell macht einige der weltweit beliebtesten Anwendungen und Dienste angreifbar, da das Framework Log4j auf Millionen von Servern verwendet wird. Die jetzt entdeckte Server-Schwachstelle ermöglicht es Angreifenden, auf dem Zielsystem einen eigenen Programmcode auszuführen und so den Server zu kompromittieren.
Das BSI hatte die IT-Bedrohungslage für Geschäftsprozesse und Anwendungen im Dezember zunächst als extrem kritisch eingestuft und die höchste Warnstufe "rot" ausgesprochen. Mittlerweile hat sich die Lage etwas entspannt, die Warnstufe wurde daher von „rot" auf „gelb" herabgesetzt.
Weitere Informationen dazu direkt beim BSI unter:
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549177-1032.html

## Sicherheitsrisiko Mensch

Ob Pishing-Mails, unsichere Passwörter oder die unbedachte Anbindung des Büro-Laptops an infizierte Hardware – die sicherste Technik kann nicht verhindern, dass Anwender Fehler machen. Vor allem die Corona-Krise, in der für viele Mitarbeiter plötzlich das Wohnzimmer zum Arbeitsplatz wurde, wirkte hier wie ein Brandbeschleuniger: Seit Beginn der Pandemie hat es laut Bitkom in 59 Prozent der Unternehmen, in denen Angestellte im Homeoffice arbeiten, IT-Sicherheitsvorfälle im Zusammenhang mit Heimarbeit gegeben. In 24 Prozent dieser Unternehmen sogar häufig.

**Schäden durch Homeoffice**

Dass viele Mitarbeiter in der Pandemie verstärkt von zu Hause gearbeitet haben, hat zu einer enormen Steigerung der wirtschaftlichen Schäden durch Cyberkriminalität beigetragen. Nach Angaben des Instituts der Deutschen Wirtschaft Köln waren 2020 rund 52,5 Mrd. Euro Schaden auf Angriffe im Homeoffice zurückzuführen, 31 Mrd. Euro mehr als vor der Pandemie.




*geschätzte Werte Quelle: eigene Berechnungen basierend auf Bitkom (2021, 2020)



GUS ERP
GUS Group

## Sicher zu Hause arbeiten

Vor dem Hintergrund, dass das Homeoffice auch nach der Pandemie ein fester Bestandteil der Arbeitswelt bleiben wird, sollten Unternehmen hier wenn nötig nachsteuern: Regelmäßige Sicherheitsschulungen, sichere Passwörter und klar definierte Nutzer- und Berechtigungsregelungen sollten auch beim Arbeiten von zu Hause zum Standard gehören.
Stets aktuelle Authentifizierungsprozesse legen zudem genau fest, welche Daten in einem ERP-System ein Mitarbeiter nur lesen und welche er auch verändern oder mit anderen verknüpfen darf. Auf diese Weise lässt sich das Risiko von Datendiebstahl oder -manipulation durch die Mitarbeiter deutlich verringern. Mobile Arbeitsplätze sollten zudem über eine technisch aktuelle Ende-zu-Ende-Verschlüsselung oder besser noch eine Multi-Faktor-Authentifizierung verfügen.

## Technische Absicherung

Auf der technischen Seite bieten sich noch eine ganze Reihe weiterer Maßnahmen an, um ERP-Systeme vor Angriffen zu schützen:

Unternehmen, die ihre ERP-Lösung aus der Cloud beziehen, sollten zunächst das Sicherheitskonzept des Anbieters genau studieren. Zu den wesentlichen Fragen gehören dabei: Werden die Daten zwischen Cloud-Server und dem jeweiligen Endgerät des Anwenders verschlüsselt übertragen? Befinden sich die Server in einem zertifizierten Rechenzentrum, so dass eine regelmäßige ausfallsichere und verschlüsselte Datenspeicherung, Zutrittskontrollen, die Überwachung der Systeme, Brandschutz und Redundanz gesichert sind?
In diesem Zusammenhang geben Zertifizierungen in der Regel Aufschluss, wie beispielsweise die ISO9000-Serie zum Qualitätsmanagement oder die ISO27001-Zertifizierung für sichere Rechenzentren. Anbieter, die sich bei Sicherheitsfragen nicht gerne in die Karten schauen lassen, sind mit Vorsicht zu genießen.

Bei Prozessen, die den Datenaustausch zwischen verschiedenen Plattformen oder zwischen On-Premises- und Cloud-Lösungen betreffen, sind die Anwender-Unternehmen selbst gefordert, auf regelmäßige Updates und neue Features zu achten und deren Auswirkungen auf die IT-Landschaft im Blick zu behalten. Auch regelmäßige Security-Audits und Penetration-Tests sollten zum Standard gehören.

Um Lecks wie log4shell rechtzeitig zu erkennen, sollten Softwareanbieter ihre Open Source-Komponenten regelmäßig auf Schwachstellen untersuchen und die einsetzten Bibliotheken (dependency checks) hinsichtlich vulnerabler Codes prüfen. Entsprechend ist auch die Schulung von Entwicklern im Bezug auf die Erstellung sicherer Codes dringend zu empfehlen.

Bei umfangreichen hybriden ERP-Landschaften setzen manche Unternehmen auch auf zentrale SIEM-Lösungen (SIEM = Security Information and Event Management). Diese überwachen ERP-Systeme automatisch und in Echtzeit. Dadurch können sie Bedrohungen unmittelbar erkennen und bieten damit einen zusätzlichen Schutz für den IT-Betrieb und die Compliance. Kontrollmechanismen, Reports und Werkzeuge für das automatisierte Compliance- und Maintenance-Monitoring bieten zusätzlich Entlastung für die IT-Sicherheitsexperten in den Unternehmen.

## Absicherung der Cloud, aber richtig

Um für den Ernstfall gewappnet zu sein, setzen mittlerweile nicht nur große Unternehmen, sondern auch viele Mittelständler auf Backup-Systeme aus der Cloud. Sie speichern dort besonders sensible Backup-Daten oder spiegeln sogar ihre komplette Infrastruktur. Wir empfehlen, solche Lösungen von Spezialisten konzipieren und betreuen zu lassen. Ergänzt um regelmäßige Fortbildungen der Administratoren und regelmäßige Security Checks.

**Kleine Unachtsamkeit mit großen Folgen**

Was eigentlich als Sicherheitsmaßnahme gedacht ist, kann bei falscher Ausführung auch ins Gegenteil umschlagen. Eines der bekanntesten Beispiele ist der Fall der Autovermietung Buchbinder. Die IT-Abteilung des Konzerns hatte gewissenhaft tägliche Backups auf einem externen Server angelegt. Doch dort war fatalerweise ein Port offen, der Datenübertragungen per SMB (Server Message Block) erlaubt.
Rund drei Millionen Kundendaten, darunter auch Adressen und Telefonnummern von Prominenten, Spitzenpolitikern, Botschaftsangehörigen und Mitarbeitern von Bundesministerien, waren so über Wochen ungeschützt auf einem Server verfügbar. Alles, was ein Angreifer tun musste, war die passende IP-Adresse in den Browser einzugeben. Anschließend konnten rund zehn Terabyte Daten heruntergeladen werden. Ein Passwort benötigte man dafür nicht.

## Für den Fall der Fälle

m Ernstfall sind klare Verantwortlichkeiten das A und O. Ein stets aktuelles Sicherheitskonzept und eine Notfall-Liste mit den entsprechenden Kontaktdaten sollten daher immer aktuell und für sämtliche Mitarbeiter verfügbar sein, die mit dem ERP- und allen angeschlossenen Systemen arbeiten. Idealerweise umfassen Notfallpläne nicht nur den eigenen Betriebsablauf, sondern beziehen auch Lieferanten und wichtige Kunden mit ein, beispielsweise in Form spezifischer Handlungsanweisungen. Empfehlenswert ist auch eine Liste mit alternativen Lieferanten, sollten bestehende nicht mehr verfügbar sein.

Ein Notfallplan ist ein lebendes Dokument. Es muss regelmäßig aktualisiert und an veränderte Bedingungen angepasst werden. Und: Der beste Notfallplan ist nutzlos, wenn die Mitarbeiter ihn im Ernstfall nicht finden. Das Dokument sollte daher an einer zentralen Stelle abgelegt werden, die für alle Mitarbeiter leicht zugänglich ist.

Trotz aller Vorsicht: Absolute Sicherheit ist in einer ERP-Welt, in der hybride und vernetzte Systeme der Normalfall sind, nicht möglich. Aber mit den geeigneten Maßnahmen lässt sich die Erfolgsquote von Hackern zumindest stark verringern. Und das spart im Ernstfall nicht nur Nerven, sondern auch eine Menge Geld.

## Sicherheits-Checkliste

* Im Home-Office sind regelmäßige Sicherheitsschulungen, Passworthygiene und klar definierte Nutzer- und Berechtigungsregelungen genauso wichtig wie im Büro.

* Wenn Ihre Mitarbeiter mobil arbeiten, achten Sie unbedingt auf eine technisch aktuelle Ende-zu-Ende-Verschlüsselung oder eine Multi-Faktor-Authentifizierung.

* Schauen Sie sich das Sicherheitskonzept Ihres Cloud-Anbieters genau an: Zertifizierungen, wie die ISO9000-Serie zum Qualitätsmanagement oder die ISO27001-Zertifizierung für sichere Rechenzentren gehören heutzutage zum Standard.

* Für Prozesse, die den Datenaustausch zwischen verschiedenen Plattformen und Anbietern betreffen, sind Sie selbst zuständig. Behalten Sie regelmäßige Updates und neue Features sowie deren Auswirkungen auf die IT-Landschaft im Blick und sorgen Sie für eine regelmäßige Risikobewertung. Ebenso wichtig: Security-Audits und Penetration-Tests.

* Softwareanbieter sollten ihre Open Source-Komponenten regelmäßig auf Schwachstellen untersuchen und einsetzte Bibliotheken (dependency checks) hinsichtlich vulnerabler Codes im Blick behalten.

* Bei hybriden ERP-Landschaften können zentrale SIEM-Lösungen unterstützen. Sie überwachen Ihre ERP-Systeme automatisch und in Echtzeit und erkennen Bedrohungen unmittelbar.

* Backup-Lösungen sollten unbedingt von Spezialisten konzipiert und betreut werden. Empfehlenswert sind zudem regelmäßige Security Checks und Fortbildungen der Administratoren.

* Für den Fall der Fälle sorgen Sie für ein stets aktuelles Sicherheitskonzept und eine Notfall-Liste mit allen wichtigen Kontaktdaten.