handwerk.magazin
www.handwerk-magazin.de

Anleitung:

ERP-SICHERHEIT:

System vor Hackern schützen

Quelle: **GUS ERP /** https://gus-erp.com/

Im 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.

Diese 8 Punkte sollten Sie regelmäßig überprüfen:

1. Im **Home-Office** sind **regelmäßige Sicherheitsschulungen**, Passworthygiene und klar definierte Nutzer- und Berechtigungsregelungen genauso wichtig wie im Büro.
2. Wenn Ihre **Mitarbeiter mobil arbeiten**, achten Sie unbedingt auf eine **technisch aktuelle Ende-zu-Ende-Verschlüsselung** oder eine **Multi-Faktor-Authentifizierung**.
3. 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.
4. 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.
5. Softwareanbieter sollten ihre **Open Source-Komponenten** regelmäßig auf Schwachstellen untersuchen und eingesetzte Bibliotheken („dependency checks") hinsichtlich vulnerabler Codes im Blick behalten.
6. Bei **hybriden ERP-Landschaften** können zentrale SIEM-Lösungen unterstützen. Sie überwachen Ihre ERP-Systeme automatisch und in Echtzeit und erkennen Bedrohungen unmittelbar.
7. **Backup-Lösungen** sollten unbedingt von Spezialisten konzipiert und betreut werden. Empfehlenswert sind zudem regelmäßige Security Checks und Fortbildungen der Administratoren.
8. Für den Fall der Fälle sorgen Sie für ein stets **aktuelles Sicherheitskonzept** und eine **Notfall-Liste** mit allen wichtigen Kontaktdaten.