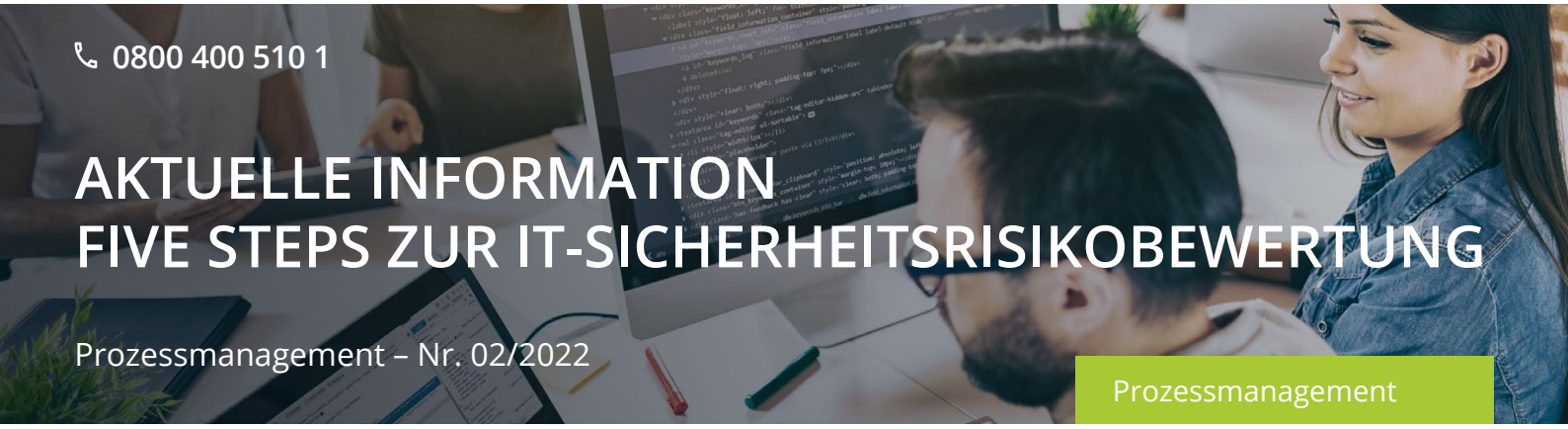


0800 400 510 1

AKTUELLE INFORMATION
FIVE STEPS ZUR IT-SICHERHEITSRISIKOBEWERTUNG

Prozessmanagement – Nr. 02/2022

Prozessmanagement

Wir entlasten Führungskräfte und schützen Mitarbeiter. Seit 1997.

Five Steps zu einer IT-Sicherheitsrisikobewertung

Cyberangriffe sind heutzutage längst im Alltag der Unternehmen angekommen. Diese treffen sowohl große Unternehmen als auch mittelständische. Daher ist es unabdingbar, sich im Rahmen eines Risiko-Managements auch hier um eine passende IT-Sicherheitsstrategie Gedanken zu machen und geeignete Schutzmaßnahmen einzuführen. Flankierend dazu und als Ergänzung zu einem bestehenden Managementsystem, etwa einem zertifizierten Qualitätsmanagementsystem, kann hier die Einführung oder Anlehnung an ein **Informationssicherheitsmanagementsystem gem. ISO/IEC 27001** erwogen werden.

Folgen von Cyberangriffen sind vielfältig und oft von **sehr hoher Gefährdung** für das Unternehmen, daher sollte hier rechtzeitig in eine starke IT-Risikomanagementstrategie investiert werden.

Im Jahr 2021 war ein immenser Anstieg des Online-Handels zu beobachten. Bereits im ersten Halbjahr gaben Käufer online 45,2 Milliarden Euro für Waren und Dienstleistungen aus. Viele Unternehmen stellten sich hier auf E-Commerce ein, um die Chance auf eine neue Einnahmequelle zu nutzen oder ihr Angebot zu erweitern. Viele Kleinunternehmen boten hier unbewusst **neue Angriffsflächen** für Cyber-Angreifer. Vermutlich geschah dies oft unwissentlich, weil der Umgang mit Online-Shops ungewohnt war. Folgen können hier bei einer IT-Sicherheitsverletzung hohe Strafen und Reputationsschädigung sein. Dies kann für kleine und mittelständische Unternehmen das Aus bedeuten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht hierbei davon aus, dass eine von vier Cyberattacken **sehr schwere, wenn nicht gar existenzbedrohende Folgen hat**.

Weitere Untersuchungen wie der Data Breach Investigation Report zeigen, dass die Attacken bei KMUs in etwa gleich viele wie bei größeren Firmen sind (263 KMU, 307 große Unternehmen). Um so wichtiger ist es daher, dass hier nach Kontrolle der Ausgaben sowie der Sicherheitsprotokolle und des IT-Risikomanagements, Investitionen in die IT-Sicherheit und Verständnis für das Risikomanagement getätigt werden. Im Anblick der Komplexität ein fast unmögliches Unterfangen.

Unerlässlich sind hier die Einführung neuer **Arbeitsrichtlinien** sowie die Prüfung der ausführlichen **IT-Strategie**, um erhebliche Betriebsunterbrechungen zu verhindern oder auch ggf. einen schnellen Wiederanlauf zu ermöglichen.
Daher heute unsere Five Steps zur erfolgreichen Umsetzung einer IT-Sicherheitsstrategie.

Leistungsangebot Prozessmanagement

AKTUELL & WICHTIG!
Krisenmanagement- und Prozessmanagement Beratung

Potentiale identifizieren & analysieren

Strukturen entwickeln & gestalten

Prozesse festlegen & zielgerichtet steuern

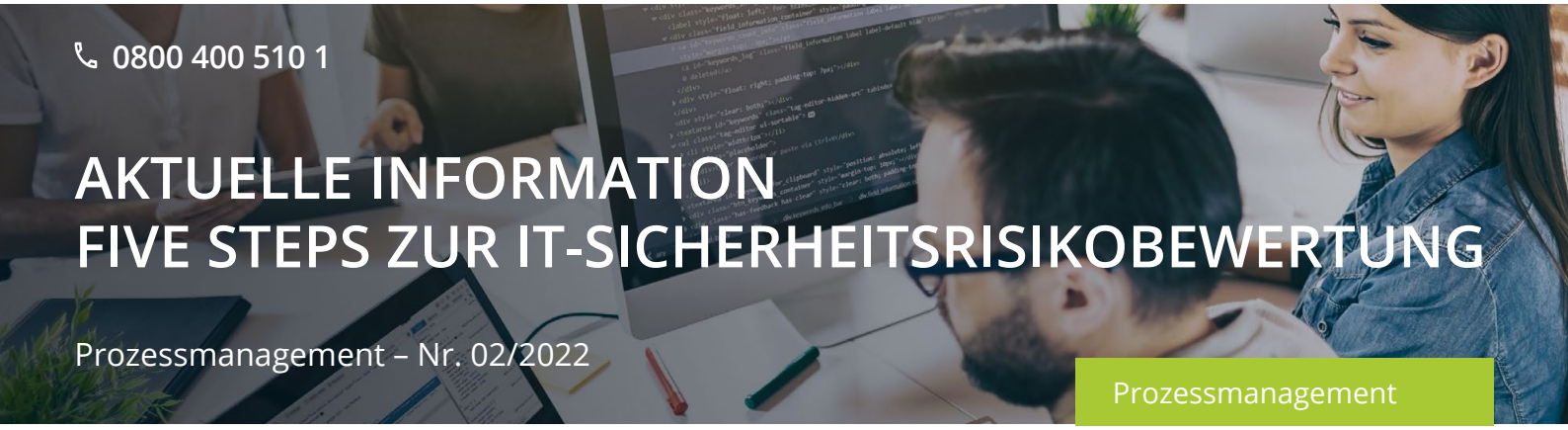
Lifecycle & nachhaltige Entwicklung

Managementsysteme - QHSE

WIE KÖNNEN WIR IHNEN HELFEN?

FKC CONSULT GmbH
Eschenburgstr. 5
23568 Lübeck
www.fkc-gmbh.de

prozessmanagementanfrage@fkc-gmbh.de



0800 400 510 1

AKTUELLE INFORMATION
FIVE STEPS ZUR IT-SICHERHEITSRISIKOBEWERTUNG

Prozessmanagement – Nr. 02/2022

Prozessmanagement

Step 1: IT-Management verstehen

Der erste Step ist die Verbesserung des Verständnisses für Risiken in der Cyberwelt. Von erheblicher Bedeutung ist hierbei herauszufinden, wo Betriebsabläufe gestört werden können und diese Risiken zu bestimmen. Dies kann unter Umständen sehr komplex werden. Zu diesem Zweck gibt es jedoch bereits Vorschriften und Regelwerke, welche zur Verfügung gestellt werden. Hierzu gehört zum Beispiel der **Standard nach ISO 27001** und weitere Rahmenwerke. Sie sind eine **wertvolle Hilfe** zur Klärung geschäftlicher Verpflichtungen und zum Schutz betrieblicher Abläufe. Auch gibt hier das Bundeamt für Sicherheit in der Informationstechnik (BSI) gute Orientierungshilfen.

Best Practice: Sicherheitstechnologien sollten hier klar aufzeigen, wie sie die Anforderungen relevanter Compliance-Vorgaben erfüllen.

Step 2: Reduzierung der Angriffsoberfläche durch den Schutz von User-Accounts

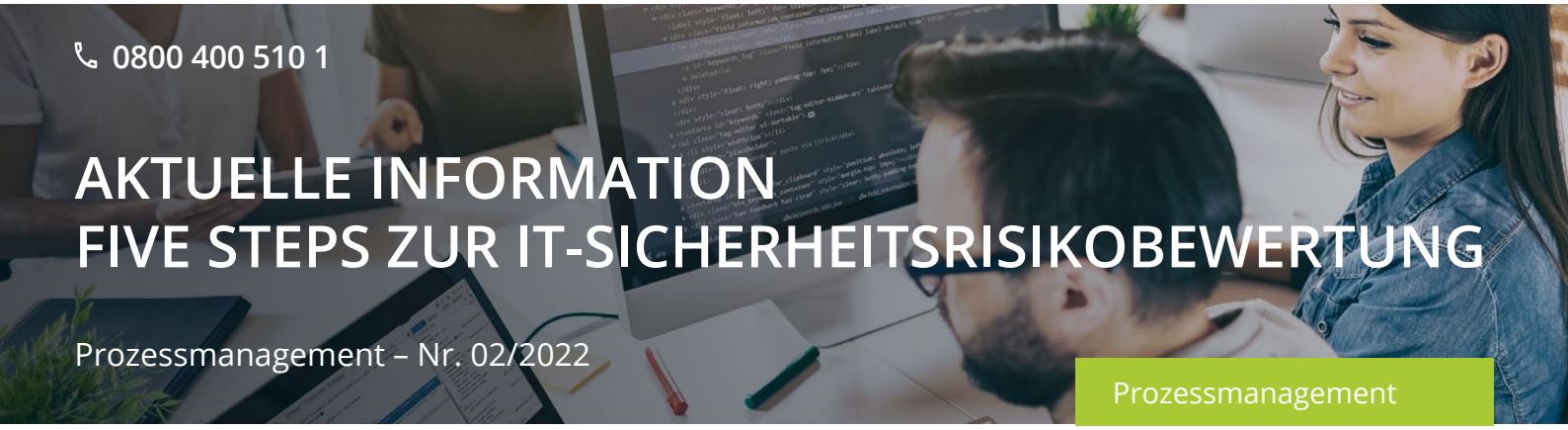
Die Überwachung und der Schutz der Benutzerkonten sind als IT-Risiko als oberstes Risiko anzusehen. So stellen z. B. die sogenannten „Privilegierten Rechte“ für externe Dienstleister, interne Administratoren, welche also auf IT-kritische Systeme zugreifen können, ein **ideales Ziel für Angreifer** dar. Hier ist es möglich mit dem Zugriff auf bereits ein Konto Daten abzugreifen, zu manipulieren, zu verschlüsseln oder gar in weitere tiefere Strukturen einzudringen. Daher sollte auch hier ein Verständnis vorhanden sein, welches unter Nutzung bestimmter Tools Schutz bringt.

Best Practice: Zugangsdaten zu kritischen Systemen sollten nicht allen Benutzern bekannt sein und stattdessen in einer sicheren „Password Vault“ aufbewahrt und regelmäßig rotiert werden. Zur sicheren Benutzer-Authentifizierung sollten Technologien wie MFA (Multi-Faktor-Authentifizierung) eingesetzt werden.

Step 3: Reduzierung der Angriffsoberfläche durch den zusätzlichen Schutz von kritischen Systemen

Der Umgang mit hochkritischen Systemen – insbesondere durch privilegierte Benutzer – geht immer einher mit einem sehr hohen Risiko, da durch fehlerhaftes Handeln (vorsätzlich oder unbeabsichtigt) ein immenser Schaden entstehen kann, wie z. B. vollständiger Systemausfall, Infektion mit Schadcode oder der Abfluss vertraulicher Daten.
Daher ist also sicherzustellen, dass im Umgang mit kritischen Systemen die entsprechenden Sicherheitsvorgaben nicht verletzt werden und lückenlos nachvollziehbar sind. So ist es z. B. möglich, dass manipulative Eingriffe auf die Datenintegrität sofort erfasst, unterbunden und gemeldet werden.

Best Practice: Anhand von Risikoklassen müssen konkrete Regelwerke definiert und umgesetzt werden, die den Aktionsrahmen auf kritischen Systemen in Echtzeit kontrollieren und bewertbar machen.



0800 400 510 1

AKTUELLE INFORMATION
FIVE STEPS ZUR IT-SICHERHEITSRISIKOBEWERTUNG

Prozessmanagement – Nr. 02/2022

Prozessmanagement

Step 4: Reduzierung der Angriffsoberfläche durch Anwendung der geringsten Privilegien

Um sicherzustellen, dass Benutzer die IT-Infrastruktur nicht schädigen können, besteht eine Möglichkeit im Entzug der zugeteilten Privilegien auf Benutzer-, Applikations- oder gar Prozessebene. Hierbei gilt es zu beachten, dass dies aber meist erhebliche Auswirkungen auf die Produktivität der Benutzer hat, wenn auf einmal die Zugriffsberechtigungen zu wichtigen Ressourcen nicht mehr ausreichen. Um die Produktivität nicht unnötig einzuschränken, sollten die Sicherheitsmaßnahmen angemessen sein.

Um hier Sicherheit und Produktivität in Balance zu bringen, empfiehlt es sich hier das **Prinzip der Privilegien mit der geringsten Notwendigkeit** anzuwenden (POLP, principle of least privileges). Basierend auf Benutzer- und Systemprofilen werden nur die Privilegien erteilt, die für die reibungsfreie Arbeit erforderlich sind, ohne Einschränkungen hinnehmen zu müssen.

Best Practice: Die Benutzerrechte von offiziellen Business Applikationen sollten durch allgemein gültige Regelwerke an Benutzer- und Maschinenprofile definiert und angewendet werden.

Step 5: Es gilt Zero-Trust

Ein automatisches Vertrauen ist unangebracht. Nicht einmal bei privilegierten Benutzern – denn Mitarbeiter mit hohen Privilegien können den falschen Befehl auf dem falschen kritischen System ausführen. Zudem besteht hier eine Anfälligkeit für raffinierte Betrügereien wie Phishing-Versuche. Auch sollte man nicht außer Acht lassen, dass es auch Mitarbeiter gibt, welche sich am Unternehmen rächen wollen und somit zum Sicherheitsrisiko werden.

Grundsätzlich gilt daher:

- Benutzer müssen immer sicher identifiziert werden (Nachweis durch starke Authentifizierung)
- Benutzer müssen sich an die Hausordnung halten (klar definierte Regelwerke, die auf der Kritikalität „Risikoklasse“ des zu schützenden Systems angewandt werden müssen).

Best Practice: Als Erstes sollte eine Klassifizierung der kritischen Systeme durchgeführt werden (Risikoklasse 0: sehr hohes Risiko – maximale Einschränkung beim Zugriff darauf). Danach sollten die Regelwerke für die Risikoklassen definiert und umgesetzt werden.

Wenn Sie sich hier als Unternehmen mit dem IT-Risiko auseinandersetzen, können Sie für die Zukunft gewappnet sein. Besonders kleinere Unternehmen, welche anfälliger für Cyber-Angriffe sind und daher Folgen sehr gravierend sein können, sind hier gefordert durch **rechtzeitiges Investieren in eine effektive IT-Sicherheitsstrategie.**
Schützen Sie Ihre Informationen durch rechtzeitiges Handeln und sprechen Sie uns gerne an, um die Möglichkeiten – gerade für KMU - die ein Informationssicherheitsmanagementsystem und eine systematische Risikobehandlung Ihnen bieten kann.
Ihr FKC Prozessmanagement-Team hilft Ihnen gerne.

prozessmanagementanfrage@fkc-gmbh.de

Bilder von Canva.