+++ CHECKLISTE +++ CHECKLISTE +++ CHECKLISTE +++ CHECKLISTE +++ CHECKLISTE +++

CHECKLISTE: 5 MINUTEN FÜR DIE SICHERHEIT IHRES UNTERNEHMENS

GEHEN SIE AUF NUMMER SICHER!

Mit dem 5-Minuten-Check-up von Kentix können Sie sofort feststellen, ob ein Sicherheitsrisiko in Ihrer physikalischen IT-Infrastruktur vorliegt. Testen Sie anhand der folgenden 10 Fragen, ob Sie die aufgeführten Risiken überwachen und abwehren können!

KENTIX
Innovative Security

RAUM

1. Haben Sie einen speziell für die IT vorbereiteten Serverraum / ein Rechenzentrum?
RISIKO: Räume für die IT-Nutzung sollten für die besonderen Anforderungen hergestellt bzw. angepasst werden und folgende Eigenschaften haben: Brandschutztüren und entsprechende Brandschutzmaßnahmen, sichere Fenster/Türen, angepasste Stromkreise, keine wasserführenden Leitungen, keine artfremde Zusatznutzung.

+10% / 0%

BRAND

2. Bekommen Sie die Entstehung von Bränden direkt gemeldet und können Sie sofort Maßnahmen einleiten?
RISIKO: 60 % der Brände entstehen in elektrischen Anlagen bzw. Geräten und entwickeln sich langsam durch Schmorbrände. Somit stellen Elektroverteilungen, USV-Systeme, Klimaanlagen und Netzteile potentielle Gefahren für Brände dar.

+15% / 0%

KLIMA

3. Werden Sie beim Anstieg der Raumtemperatur frühzeitig informiert, um Gegenmaßnahmen einzuleiten, wissen Sie über das Raumklima Bescheid?
RISIKO: Bei Ausfall der Klimaanlage kann es zu einer Überhitzung der Server kommen; dies führt meist innerhalb weniger Stunden zu einem Totalausfall der IT. Weitere kritische Zustände sind zu hohe Luftfeuchte oder Betauung nach Klimaausfällen.

+15% / 0%

LECKAGE

4. Bekommen Sie Wasserleckagen durch Rohrbrüche oder durch einen Defekt der Klimaanlage gemeldet, bevor Schäden entstehen?
RISIKO: Das Eindringen von Wasser in Serverräume durch Hochwasser, Defekte an Heizungsanlagen, Klimageräten etc. führt zu einem Totalausfall der IT.

+10% / 0%

SPANNUNG

5. Wissen Sie im Falle eines Spannungsausfalles, wie lange dieser andauert und ob Ihre USV korrekt arbeitet?
RISIKO: Bei einem Spannungsausfall kann es zu unerwarteten Störungen der USV kommen und damit zu einem Totalausfall der IT. Spannungsschwankungen werden oft auch durch Industrieanlagen verursacht und können zu USV- bzw. Netzteilfehlern führen.

+10% / 0%

EINBRUCH

6. Haben Sie Maßnahmen getroffen, um Einbrüche zu vermeiden, und können Sie auf Einbrüche umgehend reagieren?
RISIKO: Einbruch oder Diebstahl sind die offensichtlichsten Bedrohungen. Hier kann es neben dem physischen Diebstahl von Hardware auch zu logischen Zugriffen und Attacken kommen. Offene Ports oder zugängliche Konsolen stellen kritische Angriffspunkte dar.

+15% / 0%

ZUTRITT

7. Können Sie zu jedem Zeitpunkt nachvollziehen, wer wann und wie lange im Raum war?
RISIKO: IT-Räume sind adäquat gegen unbefugte Personenzutritte zu sichern, und diese sind auch möglichst zu dokumentieren. Sehr oft finden Angriffe auf die IT aus den Unternehmen selbst statt.

+10% / 0%

AUSFALL

8. Elektronische Geräte können ausfallen; bekommen Sie Ausfälle aktiver Komponenten bzw. von Netzwerkverbindungen jederzeit, auch an Wochenenden, mit?
RISIKO: Beim Ausfall aktiver oder passiver Komponenten wie Router, Switches, Telefonanlagen kann es zu massiver Störung der IT-Infrastruktur kommen. Unternehmensausfälle von einigen Stunden können hier schnell hohe Kosten verursachen.

+5% / 0%

MENSCHLICHES FEHLVERHALTEN

9. Bekommen Sie und weitere Personen die Auswirkungen menschlichen Fehlverhaltens frühzeitig gemeldet und können diese Meldungen auch unabhängig von Ihrer IT übertragen werden, z.B. als SMS?
RISIKO: Falsche Bedienung, offene Fenster, Missachtung von techn. Anweisungen, ungeschicktes Verhalten: All dies führt regelmäßig zu teuren IT-Ausfällen. Zur Vermeidung tragen organisatorische Maßnahmen bei. Eine schnelle und redundante Benachrichtigung an mehrere Personen im Fehlerfall ist dabei wichtig.

+5% / 0%

DOKUMENTATION

10. Können Sie zu jedem Zeitpunkt Ereignisse nachvollziehen und rekonstruieren (auch über mehrere Monate), um zukünftige Fehler zu vermeiden?
RISIKO: Dokumentation und Aufzeichnung von normalen und kritischen Systemzuständen über Monate oder Jahre verlangen viele QS- und Zertifizierungssysteme. Eine lückenlose Dokumentation entbindet Sie möglicherweise von Haftungsrisiken.

+5% / 0%

IHRE PHYSISCHE IT-INFRASTRUKTUR HAT FOLGENDES SICHERHEITSNIVEAU:

ERGEBNIS: ..... %

0-30%	Mangelhafte Absicherung gegen grundlegende physische Risiken.
40-70%	Basisabsicherung, jedoch mit hohem Verbesserungspotential.
80-90%	Bereits gute Absicherung, hier sollten zur weiteren Verbesserung die fehlenden Punkte analysiert werden.
100%	Gratulation, perfekte Absicherung. Derzeit besteht kein Handlungsbedarf.