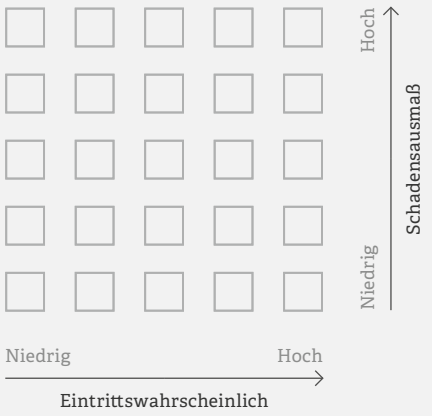
DIGITAL AGENTUR BERLIN

IT-Sicherheitscheckliste

Risikoanalyse: Technische & organisatorische Maßnahmen

Als „**technische & organisatorische Maßnahmen**“ werden alle Vorkehrungen bezeichnet, die zum Schutz von verarbeiteten Daten und Informationen getroffen wurden. Technische Maßnahmen sind bereits in technischen Geräten einprogrammiert oder eingestellt und organisatorsche Maßnahmen werden auf Anweisung oder gemäß Schulungen von den Anwendenden umgesetzt.

Anhand der folgenden Fragen können Sie bestimmte Gefährdungen in Ihrem Unternehmen einschätzen, bewerten und kategorisieren. **Je wahrscheinlicher der Eintritt eines Schadens** ist und **je höher das Schadensausmaß** wäre (je weiter oben rechts Sie ein Kreuz setzen), umso wichtiger ist es, Gegenmaßnahmen zu treffen.

Gefährdung	Risikoeinschätzung
1. Physische Sicherheit Können Ihre Geschäftsräume durch Elementarschäden (Feuer, Sturm, Übeschwemmung, Blitzschlag) zerstört oder schwer beschädigt werden oder haben Sie Sicherheitsvorkehrungen getroffen (z.B. Feuermelder, Löscheinrichtungen, Rauch-, Wassermelder)?	

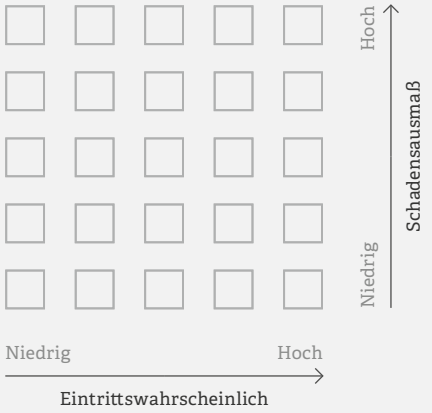
Risikoanalyse: Technische & organisatorische Maßnahmen

DIGITAL AGENTUR BERLIN

Gefährdung	Risikoeinschätzung

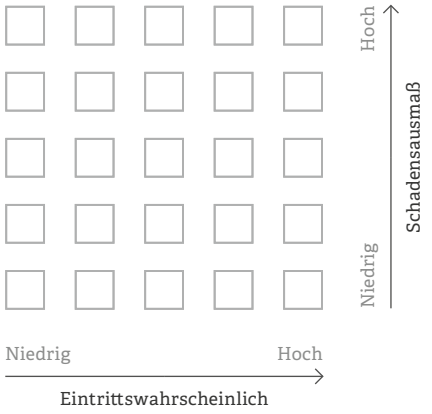
2. Technische Sicherheit

Können IT-Sicherheitsvorfälle eintreten, weil Datenverarbeitungssysteme (Computer, Laptop, Smartphone, Tablet, NAS-Speicher …) nicht dem Stand der Technik entsprechen, zu alt sind, keine regelmäßigen Updates erhalten oder nicht gewartet wurden?



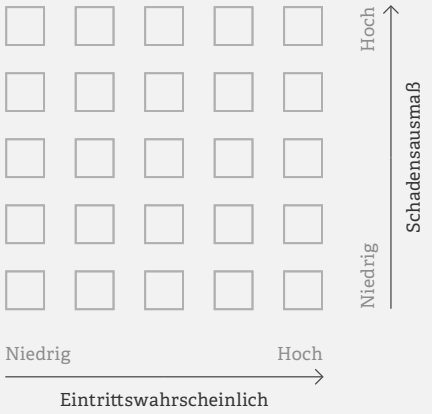
3. Zutrittskontrolle

Könnte sich jemand unberechtigt, inner- oder außerhalb Ihrer Geschäftszeiten, Zutritt zu Ihren Räumlichkeiten verschaffen oder gibt es Sicherheitsvorkehrungen (z. B. durch Zutritts- und Besucherregelungen, Einbruchsalarmierung, Wachpersonal o. ä.)?



4. Zugangs-/Zugriffskontrolle

Kann es zu unbefugtem Zugriff auf Ihre IT-Geräte kommen oder sind diese ausreichend davor geschützt (sichere Passwörter, personalisierte Nutzerkonten, Firewall, gesichertes Netzwerk, geschultes Personal usw.)?



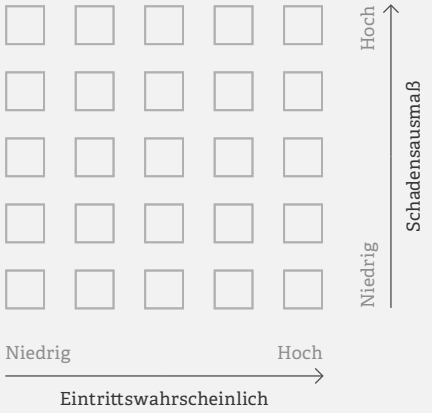
Risikoanalyse: Technische & organisatorische Maßnahmen

DIGITAL AGENTUR BERLIN

Gefährdung	Risikoeinschätzung

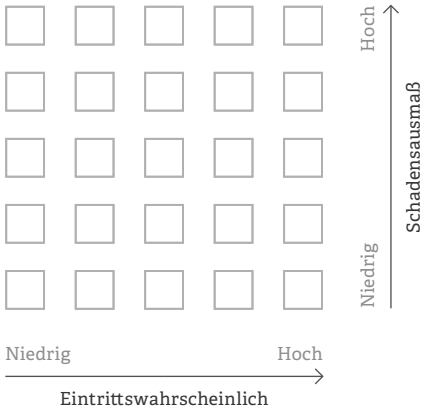
5. Weitergabekontrolle

Könnten Daten unabsichtlich oder vorsätzlich an unbefugte Dritte weitergegeben werden oder bestehen sichere Versandmethoden, wie Verschlüsselung von Daten oder Gerätespeichern, Löschprozesse, Verbot von USB-Speichern o. ä.?



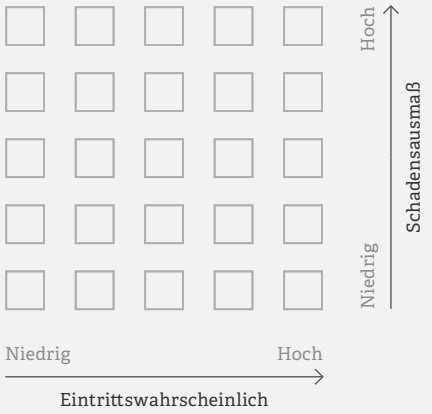
6. Eingabekontrolle

Können betriebliche Informationen außerplanmäßig (unabsichtlich oder vorsätzlich) geändert, manipuliert, gelöscht werden oder gibt es Berechtigungsstrukturen, welche Regeln dafür vorsehen oder gibt es ggf. Protokolle über alle Veränderungen (bspw. Cloud-Änderungslogs)?



7. Auftragskontrolle

Können Datenverarbeitungssysteme unabsichtlich oder fahrlässig falsch bedient und somit ein IT-Sicherheitsvorfall ausgelöst werden oder sind alle Anweisungen verschriftlich, in Form von Arbeitsanweisungen und Schulungen eigener Beschäftigter, als auch von Verträgen für externe Dienstleister?



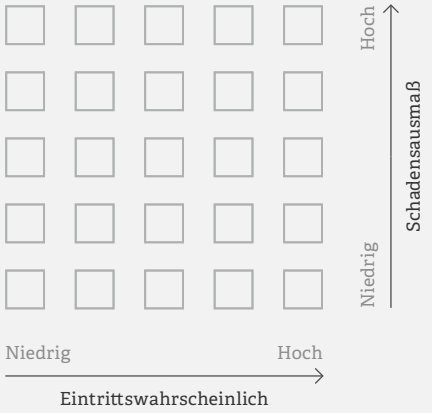
Risikoanalyse: Technische & organisatorische Maßnahmen

DIGITAL AGENTUR BERLIN

Gefährdung	Risikoeinschätzung

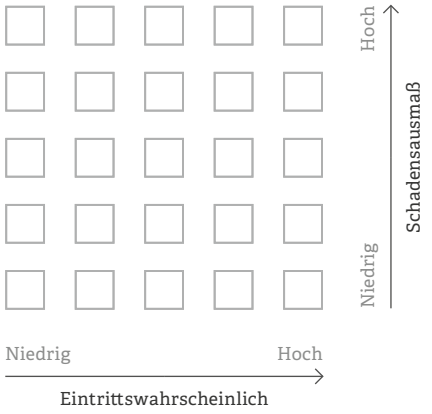
8. Verfügbarkeit / Wiederherstellbarkeit

Können Daten durch IT-Sicherheitsvorfälle unwiederbringlich zerstört oder langfristig nicht verwendbar werden oder gibt es Sicherheitskopien, die geeignet sind, Daten unterschiedlicher Zeiträume wiederherzustellen (Backup), Ersatzgeräte, Notstrom-Einrichtungen u. ä.?



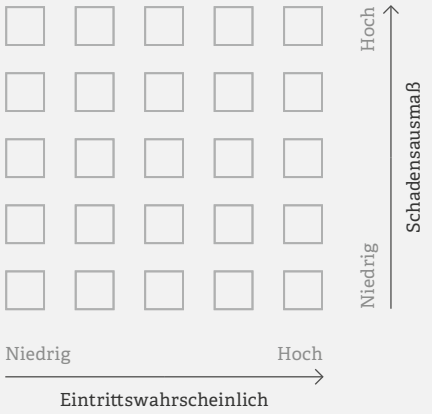
9. Trennungsgebot

Können Daten versehentlich, fahrlässig oder sogar vorsätzlich zu einem anderen Zweck genutzt werden oder sind diese technisch, räumlich, systematisch getrennt (Personalakten/Kundendaten, Dienstgeräte/Privatgeräte, abgesicherte Bereiche innerhalb des Firmennetzwerks)?



10. Sensibilisierung und Schulungen

Besteht ein Risiko, dass Mitarbeitende nicht wissen, wie sie sich in Sicherheitsnotfällen verhalten sollen und dadurch Fehler machen oder werden regelmäßige Schulungen durchgeführt und dokumentiert (Meldewege, Datenschutz, Arbeitssicherheit, Umgang mit Spam-Mails, Umgang mit Datenverarbeitungssystemen)?



Gerne unterstützen wir Sie bei der Umsetzung der Maßnahmen zur Erhöhung der IT-Sicherheit in Ihrem Unternehmen. Wir freuen uns auf Ihre Anfrage an **info@digitalagentur.berlin**.

Weitere Informationen finden Sie auch auf **digitalagentur.berlin** oder rufen Sie uns unter der **Cyberhotline 030 166 360 580** an.