Sicherheit im Ausnahmezustand

Was passiert, wenn plötzlich nichts mehr geht?

Moderne Organisationen sind hochgradig abhängig von Strom, IT und vernetzten Systemen. Fällt diese Grundlage weg, geraten Informationssicherheit, Datenschutz und physische Sicherheit gleichzeitig unter Druck.

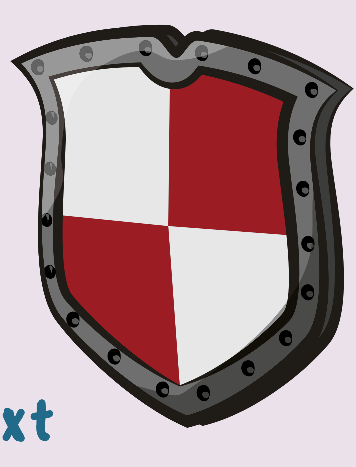
Ein Stromausfall kommt ohne Vorwarnung, ausgelöst durch technische Defekte, Extremwetter oder externe Störungen, wie zuletzt in Berlin. Was im privaten Umfeld oft nur eine Unannehmlichkeit ist und ohne Konsequenzen bleibt, wird für Unternehmen schnell zu einem ernsthaften Sicherheits-, Datenschutz- und Geschäftsrisiko. In solchen Situationen entscheidet sich, ob Sicherheits- und Datenschutzkonzepte auch unter realen Belastungen tragfähig sind. Organisationen, die ihre Abhängigkeiten kennen, klare Abläufe definiert haben und ihre Mitarbeitenden vorbereitet haben, bleiben handlungsfähig. Sicherheit ergibt sich dann aus dem Zusammenspiel technischer Vorkehrungen, belastbarer Prozesse und informierter Entscheidungen im Arbeitsalltag.

Viele Unternehmen setzen auf moderne Technik und digitale Prozesse. **Doch was passiert, wenn diese Systeme plötzlich nicht mehr verfügbar sind und auf manuelle Notlösungen zurückgegriffen werden muss?**

Vorfallmanagement im Krisenfall: Ein Zusammenspiel zwischen ISO, NIS-2 und DSGVO

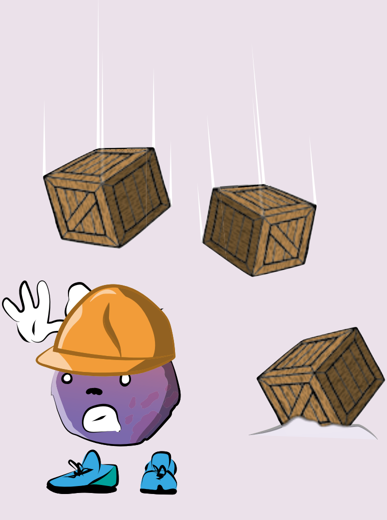
Ein strukturiertes Vorfallmanagement ist ein zentraler Baustein der **ISO/IEC 27001** und wird durch die Anforderungen der **NIS-2-Richtlinie** sowie der **KRITIS-Verordnung** weiter konkretisiert. Stromausfälle und Notsituationen sind dabei als sicherheitsrelevante Ereignisse zu bewerten, da sie die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und Systemen unmittelbar gefährden können. Gleichzeitig bleibt auch im Ausnahmezustand die Einhaltung der DSGVO verbindlich: **Sicherheitsvorfälle mit Bezug zu personenbezogenen Daten müssen erkannt, bewertet und, sofern erforderlich, fristgerecht gemäß Art. 33 und 34 DSGVO an die zuständige Behörde gemeldet werden.**

Unternehmen, **insbesondere** KRITIS-Betreiber und NIS-2-relevante Einrichtungen, müssen daher sicherstellen, dass Meldewege, Eskalationsmechanismen und Verantwortlichkeiten auch bei eingeschränkter IT- und Kommunikationsverfügbarkeit funktionieren. Ein regelmäßig getestetes, dokumentiertes Vorfallmanagement, das Datenschutz, Informationssicherheit und Betriebskontinuität miteinander verzahnt, ist entscheidend, um regulatorische Anforderungen zu erfüllen, Haftungsrisiken zu reduzieren und die Resilienz der Organisation nachhaltig zu stärken.

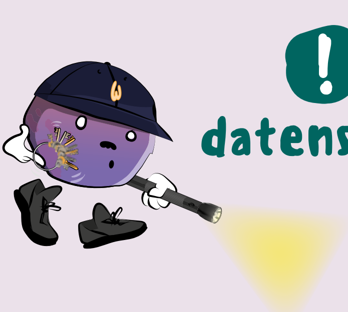


Typische Risiken bei Stromausfällen im Unternehmenskontext

- **Ausfall der Videoüberwachung:** Kameras, Aufzeichnungssysteme und Leitstellen sind ohne Notstrom nicht funktionsfähig. Sicherheitslücken entstehen, Zugriffe und Vorfälle können nicht mehr nachvollzogen werden.
- **Elektronische Zutrittskontrolle:** Türen lassen sich nicht mehr kontrolliert öffnen oder schließen. Unbefugter Zutritt kann begünstigt werden, auch in Bereichen, in denen personenbezogenen Daten oder sensible Unterlagen vorgehalten werden.
- **Smart-Technologien:** Gebäudeautomation, Alarmsysteme, Sensorik oder Cloud-Anwendungen funktionieren ohne Strom oder Netzwerk nicht. Schutzmechanismen greifen nicht mehr.
- **IT- und Datenverluste:** Server, Arbeitsplätze und Netzwerke fallen aus. Daten können verloren gehen, beschädigt oder unbefugt eingesehen werden.
- **Kommunikationsprobleme:** E-Mail, Telefonanlagen oder Kollaborationstools stehen nicht zur Verfügung. Häufig werden kurzfristig unsichere Kommunikationswege genutzt.
- **Gefährdung von Mitarbeitenden:** Dunkle Bereiche, fehlende Orientierung und unklare Zuständigkeiten erhöhen das Unfall- und Haftungsrisiko.



Warum Stromausfälle auch datenschutzrechtlich kritisch sind



- **Technische und organisatorische Maßnahmen** setzen funktionsfähige Systeme voraus
- Notlösungen sind häufig **nicht geprüft und nicht dokumentiert**
- **Zugriffsbeschränkungen lassen** sich manuell schwer kontrollieren
- Verantwortlichkeiten sind im **Ernstfall oft unklar**
- **Betroffene Personen erwarten** auch in Ausnahmesituationen einen **verantwortungsvollen Umgang** mit ihren Daten

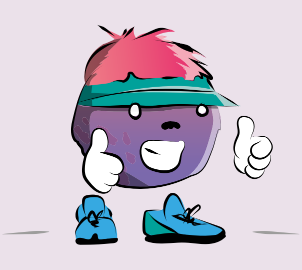
Was sollte im Voraus geklärt werden?

Es sollte, sofern möglich, vermieden werden:

- ☒ sich ausschließlich auf elektronische Systeme ohne Notfall- und Datenschutzkonzept zu verlassen;
- ☒ Notfallpläne nur theoretisch zu dokumentieren, ohne sie praktisch getestet zu haben;
- ☒ Mitarbeitende im Ernstfall ohne klare Anweisungen zum Umgang mit Daten und Informationen agieren zu lassen;
- ☒ sensible Bereiche oder Daten ohne mechanische, organisatorische oder personelle Absicherung zu betreiben.

Im besten Fall würde die Organisation:

- Notfall-, Evakuierungs- und Datenschutzkonzepte miteinander verzahnen; ✓
- klare Verantwortlichkeiten für Sicherheit, IT und Datenschutz im Krisenfall festlegen; ✓
- Notstromlösungen (z. B. USV, Generatoren) für sicherheits- und datenschutzkritische Systeme prüfen; ✓
- Backup-Lösungen für Zutritt, Dokumente und Kommunikation vorsehen; ✓
- regelmäßige Tests, Übungen und Schulungen durchführen. ✓



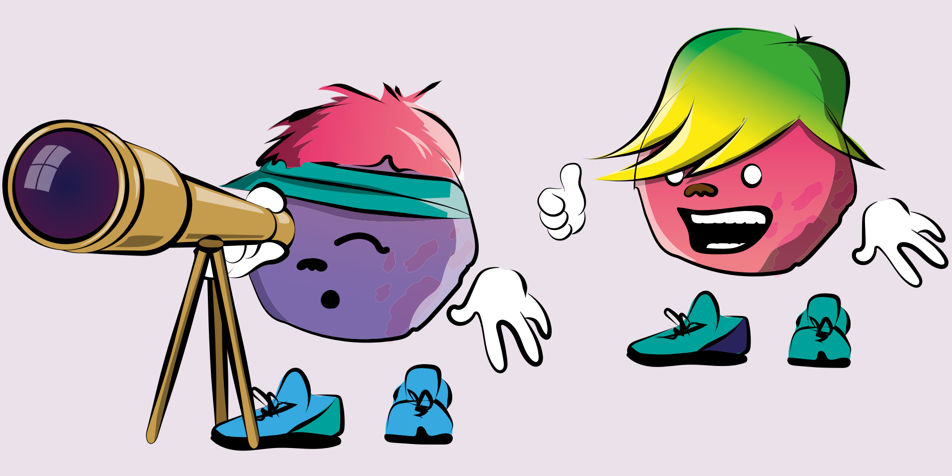
Konkrete Notfallmaßnahmen unter Berücksichtigung von Datenschutz und Informationssicherheit

Hilfreich wäre:

1. **Notstromversorgung:** Welche Systeme müssen aus Sicherheits- und Datenschutzsicht zwingend weiterlaufen (z. B. Videoüberwachung, Server, Zutrittskontrolle)?
2. **Zutrittsmanagement:** Wie wird sichergestellt, dass nur befugte Personen Zugang zu sensiblen Bereichen und Daten erhalten?
3. **Videoüberwachung:** Sind Aufzeichnung, Zugriff und Datenschutz auch im Notbetrieb geregelt?
4. **Kommunikation:** Welche datenschutzkonformen Alternativen stehen im Krisenfall zur Verfügung?
5. **Dokumentation:** Notfall- und Datenschutzmaßnahmen aktuell halten und zugänglich machen.
6. **Schulung der Mitarbeitenden:** Sensibilisierung für den sicheren Umgang mit Daten auch im Ausnahmezustand.

Fazit: Vorausschauendes Handeln schafft Sicherheit und Stabilität!

Stromausfälle und Notsituationen machen deutlich, **wie eng Sicherheit, Datenschutz und Informationssicherheit zusammenwirken**. Technische Maßnahmen entfalten ihre Wirkung nur, wenn sie in klare Prozesse eingebettet sind und durch vorbereitete Notfallregelungen ergänzt werden. Organisationen bleiben im Ausnahmezustand handlungsfähig, wenn Verantwortlichkeiten geklärt sind und Mitarbeitende wissen, wie sie sicher und datenschutzkonform handeln. **Voraussorge schützt den Betrieb und erhält das Vertrauen von Kunden, Mitarbeitenden und Geschäftspartnern.**



Dr. Bittner Consulting
GmbH & Co. KG

Podbielskistraße 386
30659 Hannover

Servicenummer: 0800 88446688
E-Mail: office@drbg.de