IT-Notfallplan

1. Allgemeine Informationen

Unternehmen: SPIEGELBLANK Reinigungsunternehmen Heinz Kuhnert GmbH & Co. KG
Branche: Gebäudereinigung / Reinigungsdienstleistungen
Adresse: Seekoppelweg 9, 24113 Kiel
Telefon (Notfallnummer): 0431-64807-5000

Notfallnummer STOIK: 0221-9567 3344
Hotline lmbit (9/5): 0431-6703-111

Ansprechpersonen im IT-Notfall:
- Volkmar Meyer – Leiter IT (IT-Verantwortlicher)
- Olaf Bremer – Geschäftsführer
- Katharina Kuhnert – Geschäftsführerin

2. Kritische Geschäftsprozesse

Die folgenden Prozesse sind für die Aufrechterhaltung des Geschäftsbetriebs kritisch:

- Faktura (Rechnungsstellung) – notwendig für Liquidität und Kundenabrechnung
- Finanzbuchhaltung – zentrale Funktion für laufende Geschäftsvorfälle und Steuerpflichten
- Lohn- und Gehaltsbuchhaltung – essenziell zur fristgerechten Bezahlung der Mitarbeitenden
- ERP-System DIGRAS – Hauptsystem zur Einsatz- und Auftragsplanung
- Betrieb der IT-Infrastruktur (Terra Xaler-Serverlandschaft) – Basis aller operativen IT-Services

3. Kritische IT-Systeme

- ERP-System DIGRAS
- Server-Infrastruktur Terra Xaler (On-Premises)
- Microsoft 365 (E-Mail, OneDrive, Teams)
- QNAP Backup-System (3-2-1-Strategie, inkl. Offline-Komponente)
- VPN- und Standortverbindungen (7 Standorte)
- USV-Systeme an allen Standorten zur Absicherung gegen Stromausfälle und Spannungsschwankungen
- Hinweis: Zugänge zu Notfallkonten sind durch besonders starke Passwörter mit einer Länge von **50 Zeichen** abgesichert. Die Passwörter erfüllen hohe Komplexitätsanforderungen und sind vor unbefugtem Zugriff geschützt hinterlegt.

4. Risikoanalyse und Notfallszenarien

Mögliche IT-Notfälle:

- Lokaler Server- oder Netzwerk-Ausfall
- Ransomware- oder Malware-Angriff
- Physische Schäden an IT-Systemen
- Ausfall des Cloud-Dienstes (Microsoft 365)
- Datenverlust durch Fehlbedienung oder Hardwaredefekt
- Social-Engineering- oder Phishing-Angriff

5. Notfallorganisation und Sofortmaßnahmen

Im Notfall gelten folgende Schritte:

- IT-Leitung (Volkmar Meyer) wird umgehend informiert.
- Betroffene Systeme werden vom Netzwerk getrennt (Isolation).
- Geschäftsführung wird benachrichtigt (Olaf Bremer / Katharina Kuhnert).
- IT-Abteilung prüft die letzten sauberen Backups und koordiniert Wiederherstellung.
- Bei Cyberangriffen erfolgt Meldung an die Cyber-Versicherung (Hiscox) und ggf. Polizei.
- Datenschutzbeauftragte Person wird eingebunden, falls personenbezogene Daten betroffen sind.
- Kommunikationsverantwortliche informieren Kunden und Mitarbeitende nach Freigabe.

Hinweis:

Alle kritischen Systeme sind über USV-Anlagen abgesichert, um bei Stromausfällen den geordneten Shutdown oder Weiterbetrieb zu ermöglichen. Die USV-Anlagen werden regelmäßig getestet und gewartet.

6. Wiederanlauf- und Wiederherstellungsplan

Prioritäten für die Wiederherstellung (Recovery Time Objectives, RTO):

1. ERP-System DIGRAS und Server-Infrastruktur Terra Xaler – innerhalb von 6 Stunden (entscheidend für Auftragsplanung, Einsatzsteuerung und operative Abläufe)
2. Finanzbuchhaltung, Faktura sowie Lohn- und Gehaltsabrechnung – innerhalb von 8 Stunden (essentiell für Abrechnung, Zahlungen und laufende Geschäftsprozesse)
3. Kommunikationssysteme (E-Mail, Teams, Telefonie) – innerhalb von 24 Stunden (wichtig, aber nachrangig gegenüber dem operativen IT-Betrieb)
4. Nicht-kritische Systeme und Services – innerhalb von 48 Stunden

Anmerkung:

Die Wiederherstellung erfolgt nach der 3-2-1-Backup-Strategie unter Nutzung der Offline-Backups. Alle Systeme sind über USV-Anlagen an jedem Standort gegen Stromausfall abgesichert. Wiederherstellungstests erfolgen mindestens einmal jährlich.

Die Wiederherstellung erfolgt anhand der 3-2-1-Backup-Strategie mit mindestens einem Offline-Backup. Regelmäßige Tests der Backup-Wiederherstellung erfolgen mindestens jährlich.

7. Kommunikations- und Meldewege

- Interne Meldung: Alle IT-Vorfälle werden an ticket@spiegelblank.de gemeldet.
- Externe Meldungen:
  * Cyber-Versicherung Hiscox (Hotline / Incident Response Team)
  * Externe IT-Dienstleister (Systemhauspartner) (lmbit / LundM / Sophos MDR)
  * Datenschutzbehörde, falls personenbezogene Daten betroffen sind (Vater IT)
  * Polizei bei Verdacht auf kriminelle Handlungen

8. Externe Partner und Kontakte

- Cyber-Versicherung: Hiscox CyberClear (Schadenhotline lt. Police)
- IT-Dienstleister/Systemhaus: lmbit GmbH / Sophos MDR
- Cloud-Anbieter: Microsoft (Microsoft 365)
- Externe IT-Forensik: [bitte ergänzen]
- Datenschutz: Vater IT

9. Dokumentation und Tests

Dieser IT-Notfallplan wird mindestens einmal jährlich überprüft, getestet und bei Bedarf angepasst. Ein vollständiger Wiederherstellungstest (Disaster-Recovery-Test) erfolgt mindestens alle 24 Monate. Die letzte Überprüfung ist zu dokumentieren.

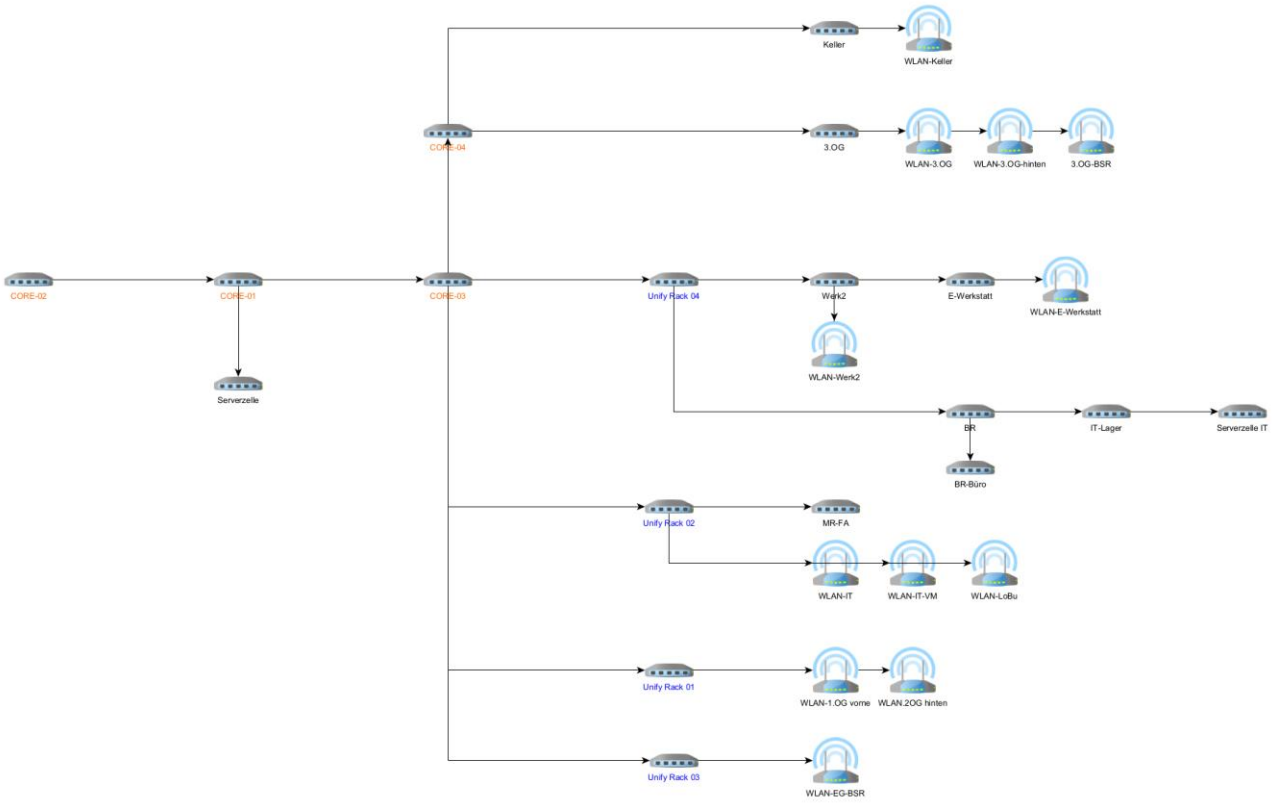
10. Anhänge

- Netzwerkplan (aktueller Stand)
- Backup-Protokolle der letzten 6 Monate
- Kontaktliste aller Schlüsselpersonen
- Checkliste für Wiederanlaufmaßnahmen

- Mail bei Angriff
-

Anhang 1 – Netzwerk- und Systemübersicht

- Standorte und Server (z. B. Terra Xaler-Systeme, ERP DIGRAS) **(in Arbeit)**
- Netzverbindungen (VPN)
- Verantwortliche IT-Kontaktpersonen
- Cloud-Dienste (Microsoft 365)

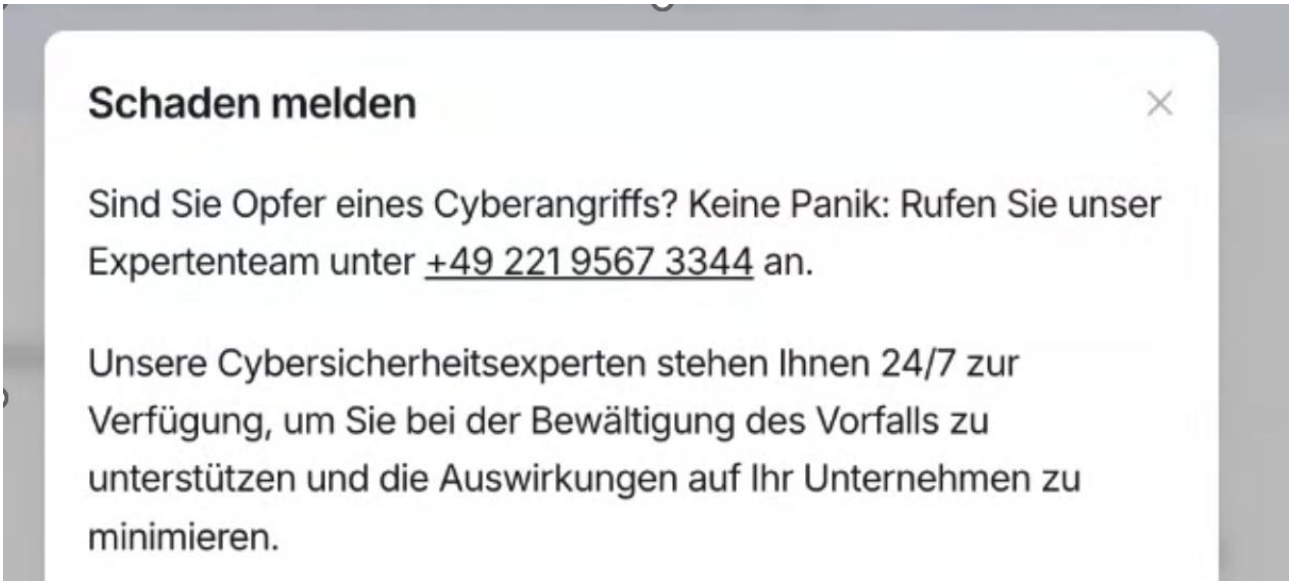


Anhang 2 – Backup-Protokoll und Wiederherstellungstest

- Datum der letzten vollständigen Datensicherung
- Backup-Typ (täglich, wöchentlich, offline)
-

- Ort der Datensicherung (lokal / Cloud / offline-Medium)
- Ergebnis des letzten Wiederherstellungstests
- Verantwortliche Person

Anhang 3 – Kontaktliste Notfallteam & Dienstleister



Rolle	**Name**	**Kontakt**	**Erreichbarkeit**
IT-Leitung	Volkmar Meyer	0431-64807-5000 0176-45672274	24/7
IT-Systembetreuung	Martin Raddai	0431-64807-5000 0152-03667772	24/7
Geschäftsführung	Katharina Kuhnert	0431-64807-15	Bürozeiten
Geschäftsführung	Olaf Bremer	0431-64807-55	Bürozeiten
IT-Dienstleister	Lmbit GmbH	0431-6703-111 helpdesk@lmbit.de	9/5
Microsoft Support	support.microsoft.com	support-eu@mail.support.microsoft.com	24/4
Sophos MDR		support@sophos.com	24/7

Anhang 4 – Checkliste Wiederanlaufmaßnahmen

Schritt-für-Schritt-Checkliste für den Ernstfall:

1. Ursache identifizieren (z. B. Strom, Hardware, Cyberangriff)
2. Betroffene Systeme isolieren
3. Backup prüfen und Wiederherstellung starten
4. Kommunikationswege aktivieren
5. IT-Dienste nach Prioritätenliste (ERP → Finanz → Mail) wiederherstellen
6. Funktionsprüfung durchführen
7. Bericht an Geschäftsleitung

Anhang 5 – Überprüfungs- und Testprotokoll

Jährlich auszufüllen:

Testdatum	**Getestet von**	**Testart**	**Ergebnis**	**Maßnahmen**
		Backup-Wiederherstellung		
		Notfallkommunikation		
		Hardware-/USV-Test		

Anhang 6 – Beispielmail

Sehr geehrte Kundin, sehr geehrter Kunde,

wir möchten Sie heute über einen IT-Sicherheitsvorfall informieren, von dem auch personenbezogene Daten betroffen sein könnten.

Was ist passiert?

Am DD.MM.YYY wurde ein unbefugter Zugriff auf unsere IT-Systeme festgestellt. Nach derzeitigem Kenntnisstand haben sich Dritte unbefugt Zugriff auf Datenbestände unseres Unternehmens verschafft. Der Angriff wurde umgehend erkannt, und unsere Systeme wurden sofort gesichert.

Welche Daten sind betroffen?

Nach unserer bisherigen Untersuchung können folgende personenbezogene Daten betroffen sein:

• z. B. Name, Adresse, E-Mail-Adresse, Telefonnummer

• ggf. Kundennummer, Vertragsdaten, Zahlungsinformationen etc.

Welche Folgen können sich daraus ergeben?

Es kann nicht ausgeschlossen werden, dass Dritte unbefugt Einsicht in Ihre Daten erhalten haben. Daraus könnten sich beispielsweise folgende Risiken ergeben:

• Missbrauch Ihrer Daten zu unbefugten Zwecken,

• Kontaktaufnahme durch Unbefugte,

• mögliche Beeinträchtigung des Datenschutzes oder der Vertraulichkeit.

Was haben wir unternommen?

Unmittelbar nach Bekanntwerden des Vorfalls haben wir:

• unsere Systeme isoliert und gesichert,

• externe IT-Sicherheits- und Forensik-Experten beauftragt,

• die zuständige Datenschutzaufsichtsbehörde informiert (gemäß Art. 33 DSGVO),

• die betroffenen Personen gemäß Art. 34 DSGVO benachrichtigt,

• zusätzliche Sicherheitsmaßnahmen implementiert, um zukünftige Vorfälle zu verhindern.

Was können Sie selbst tun?

Wir empfehlen Ihnen z. B. „auf verdächtige E-Mails zu achten“, „keine unbekannten Anhänge zu öffnen“ und uns bei Auffälligkeiten sofort zu informieren.

Unsere Kontaktstelle für weitere Informationen

Sollten Sie Fragen haben oder weitere Informationen wünschen, können Sie sich gerne an uns wenden:

Datenschutzbeauftragte: Frau Datenschutz – datenschutz@spiegelblank.de

Wir bedauern den Vorfall sehr und versichern Ihnen, dass der Schutz Ihrer Daten für uns höchste Priorität hat. Wir haben alle erforderlichen Maßnahmen ergriffen, um eine Wiederholung zu verhindern.

Mit freundlichen Grüßen