NOTFALLPLAN / -HANDBUCH “

UND SEINE AUSWIRKUNGEN

NOTFALLHANDBUCH

Begriffsdefinition

Was ist ein IT-Notfallhandbuch?

Abfallprodukt der IT-Notfallplanung

Fakten für den IT-Notfall

Hausgemachte **Lebensversicherung**

Zielsetzung

Was ist das Ziel hinter einer guten IT-Notfallplanung?

THEMENGEBIETE

- Schweregrad der Vorfalls bestimmen
- Kontaktdaten und Ansprechpartner
- Wiederherstellungsreihenfolge
- IT – Kernprozesse
- Abhängigkeiten der IT – Systeme

THEMENGEBIETE

- Wiederanlauf- und Wiederherstellungspläne kritischer IT - Systeme
- CIRP (Cyber Incident Response Plan)
- Information für den IT - Notfallstab
- Zugriff auf IT – Dokumentation und Kennwörter

SCHWEREGRAD DES VORFALLS BESTIMMEN

ESKALATIONSMATRIX FÜR NICHT-CYBERBEZOGENE VORFÄLLE
ESKALATIONSMATRIX FÜR CYBERVORFÄLLE

Die Eskalationsmatrix ist ein zentraler Bestandteil des IT-Notfallplans, der eine strukturierte Bewertung und Eskalation von Notfallsituationen ermöglicht, indem sie klare Schweregrade definiert und entsprechende Eskalationsstufen festlegt.

2.1 xEskalationsmatrix

Schweregrad	Beispiel	Eskalations-stufe 1	Eskalations-stufe 2	Eskalations-stufe 3
Störung	▪ Ausfall eines ESX- oder ESV-Hosts (und automatischem Neustart der VMs über HA). ▪ Temporärer Ausfall einer virtuellen Maschine z. B. durch fehlerhafte Windows Updates. ▪ Ausfall einer Firewall (und automatisches Failover auf die zweite Firewall).	IT-Abteilung	-	-
Notfall	▪ Ungeplanter Stromausfall für mehr als 10 Minuten. ▪ Ausfall Infor.com. ▪ Netzwerkausfall eines Core-Switches. ▪ Ausfall beider Internetverbindungen am Standorte Beerwalde. ▪ Erfolgreiches Spear Phishing bei der Geschäftsführung.	IT-Abteilung	Leitung IT-Notfallstab	-
Krise	▪ Absehbarer Ausfall von Infor.com für mehr als 24 Stunden. ▪ Insider Angriff oder Sabotage an zentraler IT-Infrastruktur. ▪ Verschlüsselung der Infrastruktur, wodurch die Produktion ausfällt *.	IT-Abteilung	Leitung IT-Notfallstab	Geschäftsführung

SCHWEREGRAD DES VORFALLS
ESKALATIONSMATRIX FÜR CYBERVORFÄLLE

Schweregrad	Beschreibung	Beispiele	Mögliche Auswirkungen	Sofortmaßnahmen	Eskalation	Kommunikationskanäle	Telefonische Eskalation außerhalb der Arbeitszeit
high	Weitreichende Cyberattacke mit katastrophalen Auswirkungen auf Systeme und Daten = Ein Major Security Incident bei Arctic Wolf.	▪ Erfolgreiche Ransomware Attacke mit Verschlüsselung zentraler Daten und Systeme. ▪ Unberechtigter Zugriff auf sensible Daten. ▪ Datenabfluss.	▪ Ausfall von zentralen IT-Ressource, die zum Ausfall von Geschäftsprozessen führen. ▪ Datenverlust. ▪ Hoher Finanzieller Schaden. ▪ Potenzieller Imageschaden.	▪ Isolierung betroffener Server und Clients (automatisch durch Arctic Wolf). ▪ Sofortige Eskalation und Aktivierung des Cyber Incident Response Plans.	IT-Administrator eskaliert sofort an: 1. Leitung IT-Notfallstab Leitung IT-Notfallstab alarmiert sofort: 1. IT-Notfallstab 2. Versicherung 3. Arctic Wolf 4. Restliche IT-Abteilung 5. Geschäftsführung	Telefon WhatsApp (Dietzel IT-Notfallstab) MS-Teams (Dietzel IT-Notfallstab) Persönlich	Ja

SCHWEREGRAD DES VORFALLS
ESKALATIONSMATRIX FÜR CYBERVORFÄLLE

Schweregrad	Beschreibung	Beispiele	Mögliche Auswirkungen	Sofortmaßnahmen	Eskalation	Kommunikationskanäle	Telefonische Eskalation außerhalb der Arbeitszeit
medium	Cyberattacke mit begrenzten Auswirkungen auf Systeme und Daten, bei dem zwar Schaden entsteht, aber kritische Systeme und Daten nicht umfassend betroffen sind.	▪ Erfolgreicher Phishing-Angriff, der zu unautorisiertem Zugriff führt, aber schnell identifiziert und gestoppt wird. ▪ Erfolgreicher Malware-Angriff auf einem Client ohne weitere Ausbreitung.	▪ Begrenzter Zugriff auf Daten oder Systeme. ▪ Abhandenkommen von Zugangsdaten und einzelnen Dateien. ▪ Keine signifikante Beeinträchtigung der Geschäftsprozesse.	▪ Überprüfung und Anpassung der Sicherheitsvorkehrungen. o Änderung der Zugangsdaten. o Aktivierung von MFA. ▪ Information der betroffenen Nutzer. ▪ Analyse des Angriffsvektors.	IT-Administrator eskaliert sofort an: 1. Leitung IT-Notfallstab Leitung IT-Notfallstab alarmiert sofort: 1. IT-Notfallstab 2. Arctic Wolf 3. Versicherung	Telefon WhatsApp (Dietzel IT-Notfallstab) MS-Teams (Dietzel IT-Notfallstab) Persönlich	Ja
low	Geringfügige Cyberbedrohung mit minimalen oder keinen tatsächlichen Schäden an Systemen und Daten.	▪ Versuch eines Malware-Angriffs, der erfolgreich von Sicherheitsmaßnahmen abgewehrt wird, ohne dass ein Eingriff erforderlich ist. ▪ Erfolgloser Phishing-Angriff.	▪ Keine oder minimale Störung. ▪ Keine Beeinträchtigung der Geschäftsprozesse.	▪ Dokumentation des Vorfalls im Dietzel Ticketsystem. ▪ Überprüfung und Anpassung der Sicherheitsvorkehrungen.	Keine Eskalation erforderlich	Ticketsystem mit Zuweisung an Admin	Nein

SCHWEREGRAD DES VORFALLS
ESKALATIONSMATRIX FÜR CYBERVORFÄLLE

Schweregrad	Beschreibung	Beispiele	Mögliche Auswirkungen	Sofortmaßnahmen	Eskalation	Kommunikationskanäle	Telefonische Eskalation außerhalb der Arbeitszeit
medium	Cyberattacke mit begrenzten Auswirkungen auf Systeme und Daten, bei dem zwar Schaden entsteht, aber kritische Systeme und Daten nicht umfassend betroffen sind.	▪ Erfolgreicher Phishing-Angriff, der zu unautorisiertem Zugriff führt, aber schnell identifiziert und gestoppt wird. ▪ Erfolgreicher Malware-Angriff auf einem Client ohne weitere Ausbreitung.	▪ Begrenzter Zugriff auf Daten oder Systeme. ▪ Abhandenkommen von Zugangsdaten und einzelnen Dateien. ▪ Keine signifikante Beeinträchtigung der Geschäftsprozesse.	▪ Überprüfung und Anpassung der Sicherheitsvorkehrungen. o Änderung der Zugangsdaten. o Aktivierung von MFA. ▪ Information der betroffenen Nutzer. ▪ Analyse des Angriffsvektors.	IT-Administrator eskaliert sofort an: 1. Leitung IT-Notfallstab Leitung IT-Notfallstab alarmiert sofort: 1. IT-Notfallstab 2. Arctic Wolf 3. Versicherung	Telefon WhatsApp (Dietzel IT-Notfallstab) MS-Teams (Dietzel IT-Notfallstab) Persönlich	Ja
low	Geringfügige Cyberbedrohung mit minimalen oder keinen tatsächlichen Schäden an Systemen und Daten.	▪ Versuch eines Malware-Angriffs, der erfolgreich von Sicherheitsmaßnahmen abgewehrt wird, ohne dass ein Eingriff erforderlich ist. ▪ Erfolgloser Phishing-Angriff.	▪ Keine oder minimale Störung. ▪ Keine Beeinträchtigung der Geschäftsprozesse.	▪ Dokumentation des Vorfalls im Dietzel Ticketsystem. ▪ Überprüfung und Anpassung der Sicherheitsvorkehrungen.	Keine Eskalation erforderlich	Ticketsystem mit Zuweisung an Admin	Nein

SCHWEREGRAD DES VORFALLS ESKALATIONSMATRIX FÜR CYBERVORFÄLLE

Schweregrad	Beschreibung	Beispiele	Mögliche Auswirkungen	Sofortmaßnahmen	Eskalation	Kommunikationskanäle	Telefonische Eskalation außerhalb der Arbeitszeit
Fehlalarm (false positive)	Fehlalarm ohne tatsächliche Sicherheitsbedrohung.	▪ Sicherheitswarnung durch Fehlkonfiguration. ▪ Antivirus meldet saubere Datei als Malware. ▪ Irrtümliche Identifikation normalen Verhaltens als verdächtig.	▪ Mögliche Ablenkung von echten Sicherheitsvorfällen.	▪ Überprüfung und Bestätigung des Fehlalarms. ▪ Anpassung der Sicherheitseinstellungen oder Regeln zur Vermeidung zukünftiger Fehlalarme.	Keine Eskalation erforderlich	MS-Teams (IT-Kanal)	Nein

Wichtig: Bei der Alarmierung ist es wichtig, sicherzustellen, dass die betreffende Person erreicht wird. Sollte ein Kommunikationskanal fehlschlagen, ist der nächste Kanal zu verwenden, bis Kontakt hergestellt ist. Bei Nichterreichbarkeit per Telefon sollte stets eine Nachricht auf der Mailbox hinterlassen werden.

MINDESTANFORDERUNGEN FÜR EINE PROFESSIONELLE REAKTION

Kontaktdaten intern + extern	Aktuelle (!) **IT-Asset Liste**	**Wiederherstellungs-reihenfolge** inkl. Abhängigkeiten	**Übersicht** der genutzten **Cloud-Dienste**
Kennwörter inkl. MFA Geräte	**Aktuelle IT-Dokumentation**	**Netzplan**	**Architektur Überblick** pro Disziplin

ABLAGEORT INFORMATIONEN DEFINIEREN

3 xKontaktdaten und Ansprechpartner

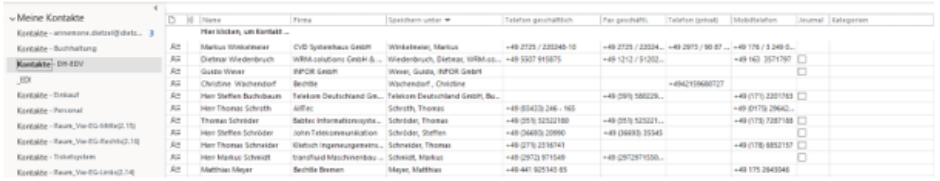
3.1 xZugriff auf interne Kontaktdaten im Normalbetrieb

Im Normalbetrieb sowie bei Ausfällen ohne die Beteiligung des Exchange Online, kann auf interne Kontaktdaten der Dietzel über Outlook Kontakte des Postfachs dh-edv@dietzel-hydraulik.de zugegriffen werden.

Dieses Postfach ist bei Annemone und David am Handy eingebunden.

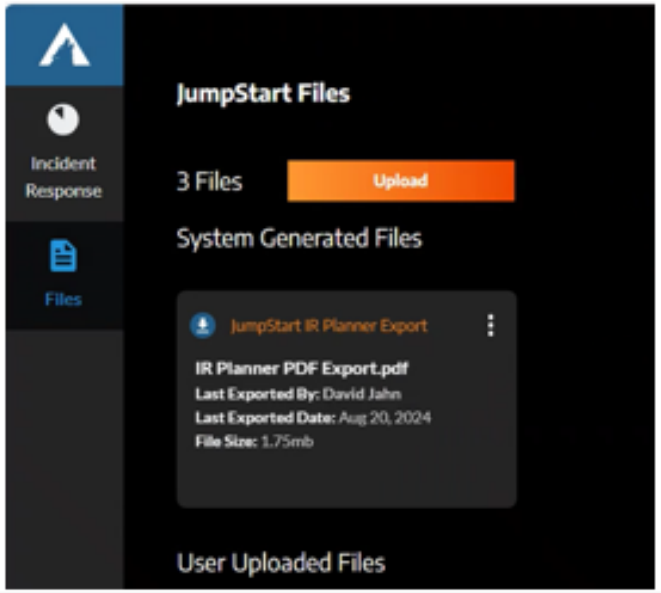
3.2 xZugriff auf interne und externe IT-notfallrelevanten Kontaktdaten im Notfall

Für den Notfall sind alle wesentlichen internen und externen IT-notfallrelevanten Kontaktdaten zentral im den Outlook-Kontakten des Postfachs dh-edv@dietzel-hydraulik.de dokumentiert. Jeder IT-Mitarbeiter hat Zugriff auf die Kontaktdaten über sein Outlook.

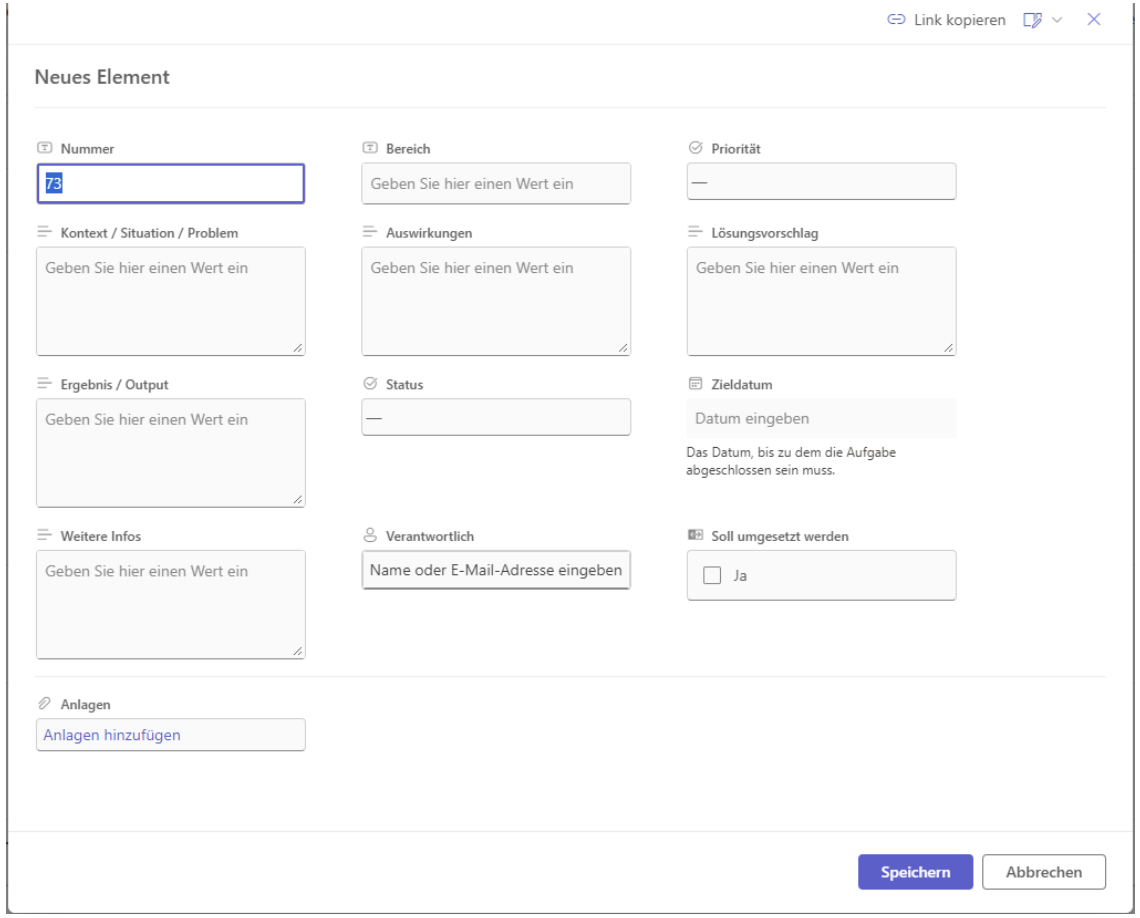


Zusätzlich werden die internen und externen IT-notfallrelevanten Kontaktdaten monatlich als CSV-Export vom IT-Notfallbeauftragten exportiert und im Arctic Wolf Portal unter *User Uploaded Files* hinterlegt.

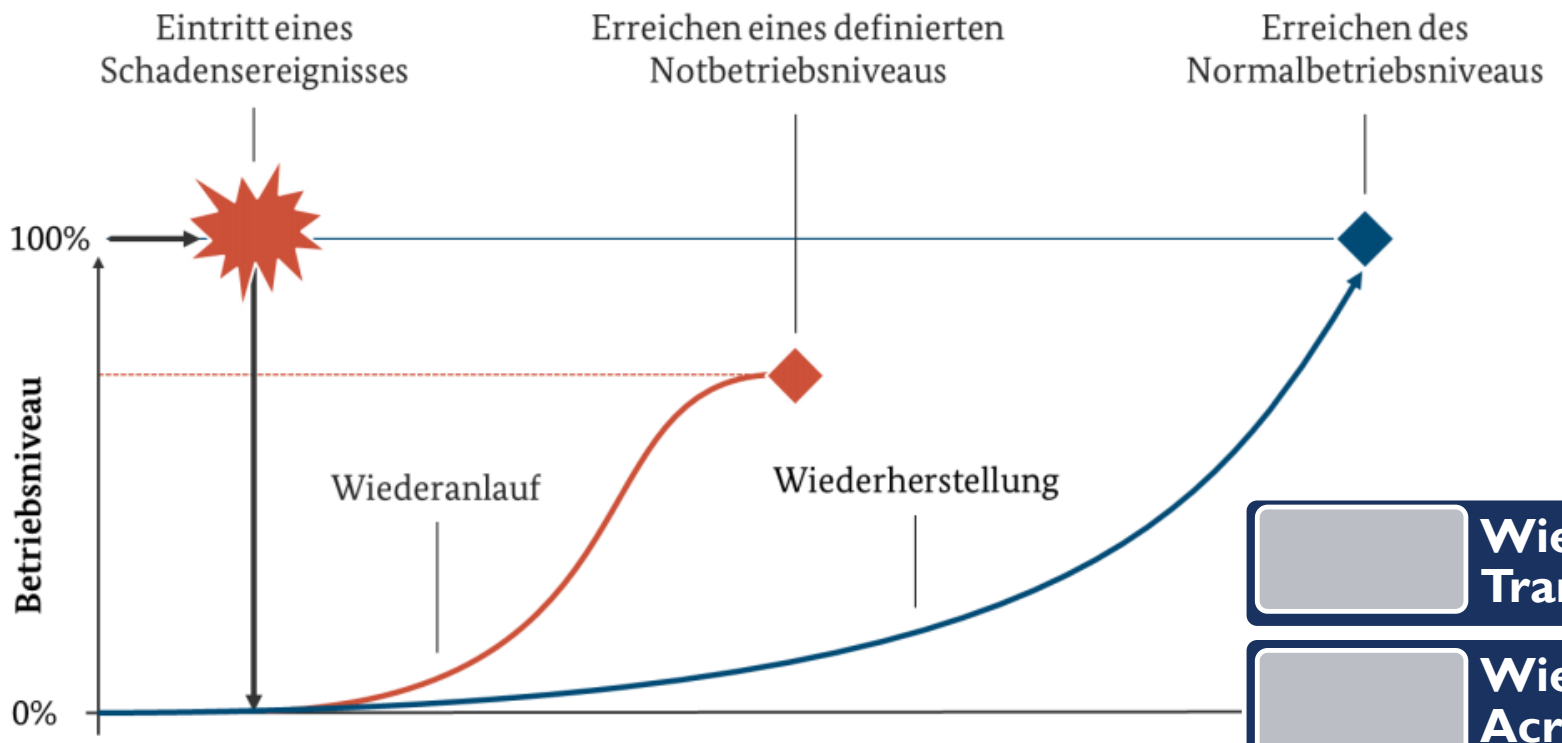
Arctic Wolf Portal: https://irplanner.arcticwolf.com/organization/2df1eebf-5ef9-4b9b-804b-ade35d645453/files



ERFASSUNG DER AUFGABEN



WIEDERANLAUF- UND WIEDERHERSTELLUNGSPLÄNE KRITISCHER SYSTEME



- **Wiederherstellung von SQL-Transaktionsbackups**
- **Wiederherstellung von VMs aus Acronis Backups**
- **Wiederherstellung von Snapshots der Pure**

5.4.6 xVoraussetzungen und Abhängigkeiten zur Wiederherstellung der VMs

Um die Wiederherstellung ausführen zu können, werden folgende Bedingungen bzw. Aktivitäten benötigt:

Eigenschaft	Erläuterung
Welche Voraussetzungen müssen grundsätzlich erfüllt werden?	▪ Strom und Klimatisierung stehen bereit ▪ Switche / Netzwerk Umgebung inkl. Firewalls stehen bereit ▪ VMware Umgebung inkl. Pure-Storage und FC-Switche stehen bereit und sind nutzbar ▪ Acronis Backup Server VM (VAAB.dietzel.local) inkl. des gewählten Backup-Storages stehen bereit und sind im Netzwerk erreichbar ▪ Mögliche Backup-Storages o NAS-BW11 o NAS-BW10

5.4.9 vHochrechnung für die benötigte Dauer der Wiederherstellung

Die folgende Tabelle enthält die benötigte Dauer für die Wiederherstellung von Sicherungen aus verschiedenen Repositories. Basierend darauf wurde eine Hochrechnung für die erforderliche Wiederherstellungszeit der gesamten Umgebung erstellt. Diese Hochrechnung beruht auf theoretischen Werten, die noch nicht durch einen Praxistest bestätigt wurden.

Bereich	Wiederherstellungsquelle	Wiederherstellungsgeschwindigkeit *	Zugewiesene \ Belegte produktive Datenmenge **	Vollbackup **	benötigte Wiederherstellungsdauer der Daten *
Virtuelle Maschinen	NAS-BW10 / NAS-BW11	201 MB/s***	85 / 41TB	3,7TB	ca. 5 Stunden und 7 Minuten
	Band-Backup	-	-		Aktuell unbekannt. Prozess muss noch definiert und getestet werden.

* Hier ist die reine Kopiergeschwindigkeit angegeben. Der Mehraufwand für administrative Aufgaben wie klicken in der Software, Entscheidungen treffen, Formatieren der Festplatten etc. ist nicht enthalten. Beim Wiederherstellungstest wurde eine VM wiederhergestellt.

CYBER INCIDENT RESPONSE PLAN (CIRP)

Die einzelnen Schritte der Schnellstartanleitung im Überblick

In der folgenden Tabelle sind Maßnahmen nach einer Cyberattacke aufgelistet. Zu jeder Maßnahme gibt es eine kurze Beschreibung, wer zuständig ist und wie lange es voraussichtlich dauert.

Maßnahme	Beschreibung	Verantwortung	Geschätzte Dauer
1. Identifikation des Vorfalls	▪ Sicherheitsvorfall feststellen.	▪ Arctic Wolf ▪ (IT-Abteilung)	ca. 30 – 60 Minuten (je nach Komplexität)
2. Triage[2] des Vorfalls	▪ Meldungen aus Sicherheitssystemen und Benutzerberichten überprüfen. ▪ Arctic Wolf Meldung vorhanden? > möglicherweise Cyberattacke. ▪ Nur Benutzerbericht oder Monitoring Meldung vorhanden? > vermutlich keine Cyberattacke. ▪ Bewerten, ob es sich um einen realen Vorfall oder um eine Fehlalarmierung (false positive) handelt. ▪ Kategorisierung des Vorfalls: „Art des Vorfalls bestimmen“ (z. B. Malware, Phishing, Ransomware, …) ▪ Durchführung einer ersten Lagefeststellung zur Bestimmung des Geltungsbereichs: Welche Systeme, Daten, Anwender, Standorte und Prozesse sind betroffen? ▪ Priorisierung des Vorfalls: Schweregrad und Dringlichkeit des Incidents (low, medium, high) bestimmen.	▪ Arctic Wolf ▪ IT-Abteilung	
3. Einleitung von Sofortmaßnahmen	▪ Dringende Sofortmaßnahmen ergreifen, um die Ausbreitung des Angriffs zu stoppen.	▪ Arctic Wolf ▪ (IT-Abteilung)	

dietzel HYDRAULIK

BECHTLE

Maßnahme	Beschreibung	Verantwortung	Geschätzte Dauer
Dokumentation	▪ Beweise sammeln, z.B. Screenshots von Fehlermeldungen erstellen oder andere relevante Informationen mit dem Smartphone abfotografieren. ▪ Alle Schritte und Ergebnisse der Vorfallreaktion sorgfältig dokumentieren, hierfür die Vorlage „Cyber Incident Response Protokoll.xlsx“ nutzen. ▪ Berichts für das Management und die beteiligten Teams erstellen.	▪ IT-Abteilung ▪ IT-Notfallstab ▪ Arctic Wolf ▪ IT-Dienstleister ▪ (ggf. Cyberversicherung)	

Hinweis: Die Zeitangeben sind geschätzt und variieren je nach Komplexität des Vorfalls.

LEITFRAGEN FÜR DAS SAMMELN & BEWERTEN VON INFORMATIONEN

6.3.1 xLeitfragen für das Sammeln & Bewerten von Informationen

Hinweis: Dieser Fragenkatalog dient lediglich als Leitfaden. Es ist nicht erforderlich, jede Frage zu beantworten.

Leitfragen	Antworten
Was ist passiert? Darstellung der Ereignisse bzw. Schäden (Was, wann, wo und wer?). Uhrzeiten des Angriffs notieren, dabei Systemzeiten und deren Abweichungen beachten. **Trennung von Wissen und Vermutung**	
Welche Maßnahmen zur Eindämmung des Vorfalles sind bereits getroffen worden?	
Betroffene Nutzer über Beobachtungen und Aktivitäten befragen. Alle Begleitumstände sind durch die Betroffenen klar, offen und ungeschönt zu erläutern.	
Konnte der Angreifer bereits ins System vordringen?	
Ist der Angriff in der in Vorbereitung, läuft noch oder bereits abgelaufen?	
Was ist die Ursache/Quelle des Schadens?	
Welche Auswirkung hat der Vorfall intern?	
Welche Auswirkung hat der Vorfall extern?	
Welche IT-Assets sind möglicherweise betroffen (Server, Clients, AD, Firewalls, Applikationen, Cloud-Dienste wie OneDrive	

ART DES VORFALLS BESTIMMEN - SOFORTMASSNAHMEN

6.4 xSofortmaßnahmen & Eindämmung

Ziel: Den verursachten Schaden schnell begrenzen, den Angreifer effektiv abschneiden und die betroffenen Systeme isolieren, um eine weitere Ausbreitung und Schädigung zu verhindern.

Oberste Regel: Keinesfalls darf eine Anmeldung mit privilegierten Nutzerkonten (Administratorkonten) auf einem potenziell infizierten System erfolgen, während das System sich noch im internen produktiven Netzwerk befindet oder mit dem Internet verbunden ist!

AUSMERZUNG

6.5 xAusmerzung

Ziel: Die Hauptursache oder den Auslöser des Vorfalls identifizieren, Malware oder Bedrohungen entfernen, die betroffenen Systeme aus der produktiven Umgebung entfernen und ähnliche Angriffe in Zukunft verhindern.

Checkliste zur Ausmerzung

- Die Ausmerzung wird gemeinsam mit dem Incident Response Team der Arctic Wolf durchgeführt. Dieses wurde im Kapitel 6.3 Lagefeststellung alarmiert.
- Das Incident Response Team der Arctic Wolf führt federführend die forensischen Analysen durch.

Folgende Aufgaben sollten in Abstimmung mit dem Incident Response Team der Arctic Wolf parallel erfolgen:

- Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüfen und absichern (z.B. neue Passwörter, 2FA).
  - Alle auf betroffenen Systemen gespeicherten bzw. nach der Infektion eingegebenen Zugangsdaten als kompromittiert betrachten und die Passwörter ändern. Dies umfasst u. a. Webbrowser, E-Mail-Clients, RDP-Verbindungen, RDP-Manager sowie andere Anwendungen wie PuTTY, WinSCP, etc.
  - Ggf. alle Kennwörter ändern

CHECKLISTE KOMMUNIKATION UND MELDEPFLICHTEN BEI CYBERVORFÄLLEN

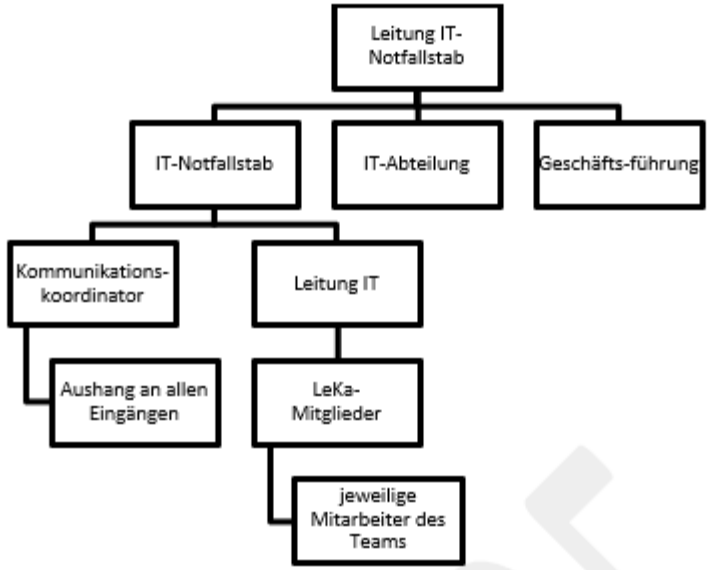
6.7 Checkliste Kommunikation und Meldepflichten bei Cybervorfällen

Hinweis

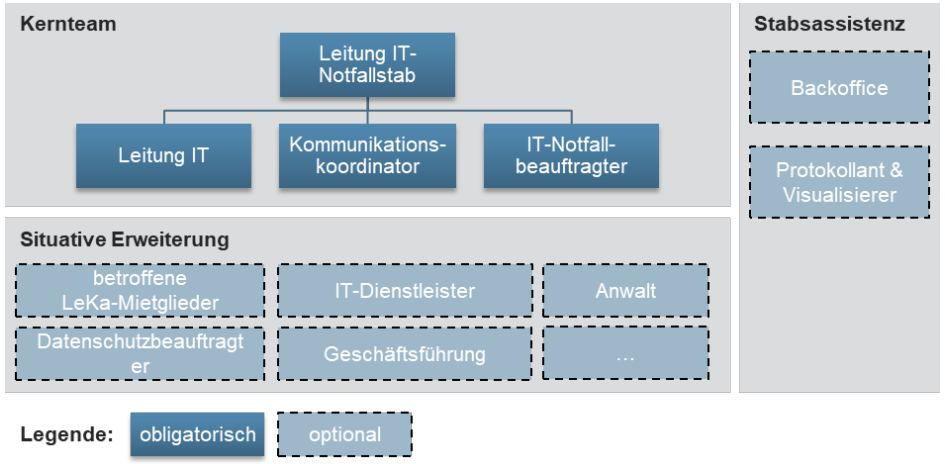
1. Die Sortierung der folgenden Liste stellt **keine Reihenfolge** dar.
2. Die Kommunikation findet fortwährend und parallel zur Bewältigung der Lage statt.

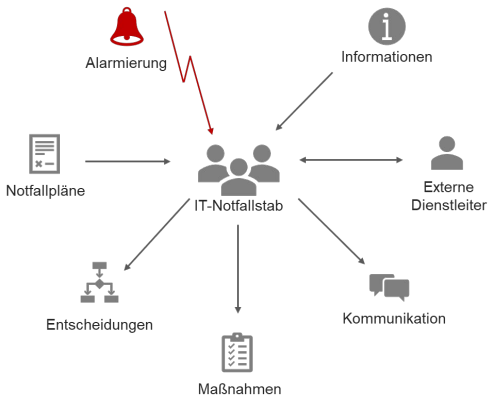
Zielgruppe	Kommunikations kanäle	Verantwortlich
Leitung IT-Notfallstab alarmieren	Telefonisch und per WhatsApp Gruppe **Dietzel IT-Notfallstab**	IT-Abteilung
IT-Notfallstab einberufen	Telefonisch und per WhatsApp Gruppe **Dietzel IT-Notfallstab**	Leitung IT-Notfallstab
Arctic Wolf Incident Reponse Team alarmieren ▪ SLA: 1-Stunde ▪ Der Vorfall muss innerhalb von 48 Stunden	+49 30 16637144	IT-Notfallstab
Wichtig: Vorher immer mit dem externen Datenschutzbeauftragten abstimmen, ob eine Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 DSGVO vorliegt.		mit der Leitung IT und Geschäftsführung
Ggf. Rechtsanwalt informieren	Telefonisch	Krisenstab
Leiter Krisenstab alarmieren	Telefonisch	Leiter IT-Notfallstab
Krisenstab alarmieren	WhatsApp Gruppe **Dietzel Krisenstab**	Leiter Krisenstab
Kommunikationsteam alarmieren	Telefonisch	Krisenstab
Kommunikationsstrategie aufstellen ▪ Was, mit wem und in welcher Tiefe kommunizieren wir? ▪ Über welche Kanäle? IT-Notfall auf der Homepage bekanntgeben?	-	Krisenstab Marketing-Abteilung
Wichtige interne Stakeholder alarmieren ▪ Gesamte Geschäftsführung ▪ Alle Betriebs- und Werksleiter ▪ Betriebsrat	Telefonisch oder persönlich	Kommunikations-team des Krisenstabs
Kommunikationskanäle für das IT-Notfallteam inkl. IT-Dienstleister definieren Mindestens folgende Optionen stehen zur Verfügung: 1. Neues Dietzel Microsoft Teams Team erstellen 2. Ad hoc neues Microsoft Teams Team bei z. B. Bechtle Austria erstellen und mit outlook.com oder privaten Adressen hinzufügen 3. WhatsApp Gruppe erstellen	-	IT-Notfallstab
Mitarbeiter informieren und IT-Notfall ausrufen **Wichtig:** Falls E-Mail nicht geht, müssen die Betriebs- und Werksleiter telefonisch die Mitarbeiter informieren. Jeder Betriebs- und Werksleiter informiert die Mitarbeiter in seinem Verantwortungsbereich. Bei nicht Erreichbarkeit Anrufbeantworter benutzen. ~~Die betrieblichen Kontaktdaten sind in der Benutzerliste.xls auf dem Notfall-USB-Stick gespeichert.~~	E-Mailverteiler oder telefonisch	Kommunikations-team des Krisenstabs oder Betriebs- und Werksleiter jeweils im Namen des Krisenstabs.

NOTFALLORGANISATION



- Die Leitung des IT-Notfallstabs alarmiert per WhatsApp Gruppe „Dietzel IT-Notfallstab“ und zusätzlich telefonisch das Kernteam des IT-Notfallstabs.
- Die Leitung des IT-Notfallstabs alarmiert per WhatsApp Gruppe „Dietzel IT-Abteilung“ und zusätzlich telefonisch die IT-Abteilung.
- Die Leitung des IT-Notfallstabs alarmiert telefonisch die Geschäftsführung. Gemeinsam wird entschieden, ob die Mitarbeiter durch die LeKa-Mitglieder darüber informiert werden, dass diese zuhause bleiben müssen und sich um 8, 12 und 17 Uhr eine Information von dem Teamleiter





ZUGEHÖRIGE DOKUMENTE

Dokument	Kurzbeschreibung
Dietzel_IT-Notfallhandbuch.docx	Ein umfassendes Dokument, das Verfahren, Verantwortlichkeiten und Ressourcen für den Umgang mit IT-Notfällen beschreibt.
Dietzel_IT-Notfallvorsorgekonzept.docx	Ein strategisches Dokument, das die Richtlinien und Maßnahmen für die IT-Notfallvorsorge im Unternehmen festlegt.
Dietzel_Informationssammlung-für-Notfallmanagement.xlsx	Eine Zusammenstellung relevanter Informationen, wie Kontaktdaten, IT-Asset Listen und Wiederherstellungsprioritäten, die im Notfall benötigt werden.
Dietzel_VORLAGE Vorfall-Dokumentation.xlsx	Eine Vorlage zur Dokumentation von Sicherheitsvorfällen.
Dietzel_Diagramme.pptx	Enthält Visualisierungen und Diagramme, die in den IT-Notfalldokumenten verwendet werden.
Dietzel_Risiken_Chancen_V1.2.xlsx	Eine priorisierte Liste der identifizierten Risiken und Chancen im Kontext der IT-Notfallplanung
Dietzel_VORLAGE Wiederanlauf- und Wiederherstellungsplan (V1.9.2).docx	Eine Vorlage zur strukturierten Dokumentation von Wiederanlauf- und

„Fünf Minuten vor der Feier
ist nicht die Zeit, um tanzen zu lernen!“

VIELEN DANK

JEMAND@EXAMPLE.COM