



Cyber-Krisenmanagement

Münster, 18. Juni 2026

Agenda

1

09:00 – 9:30

Anmeldung und Empfang

2

9:30 – 10:00

Begrüßung & Kurzvorstellung amexus

3

10:00 – 13:15

Workshop mit Kaffeepause

4

14:00 – 15:00

Networking



Speakers



Nicole Zech.

Senior Solutions Engineer

Eye Security



Erwin Musagic.

Account Executive

Eye Security



Philipp Santos de Oliveira.

Senior Cyber Security Consultant

Eye Security

Wir schützen die europäische Wirtschaft

Gegründet im Jahr 2020

Ausgliederung aus dem niederländischen
Nachrichtendienst (AIVD)

950+

Kunden

98-99%

Kundenzufriedenheit

>100%

jährliches Wachstum

Starkes Pflichtbewusstsein und Dienstbereitschaft
sind Teil der DNA

Hochqualifiziertes Spezialistenteam für offensive und defensive
nationale Sicherheit

500+

Angriffe
bei Kunden*

Direkter Kundenzugang zu Cyber-Spezialisten

SOC in Deutschland und den Niederlanden

100+

IR bei Unternehmen,
die keine Kunden
sind*

* seit 2020

Ein Blick auf die aktuelle Bedrohungslage

Business-E-Mail Compromise (BEC)



4/10

BEC-Angriffen beginnen mit einem Link
in einer E-Mail

- Die Hauptursachen waren Phishing-Links, Anhänge und servicebasierte Phishing-Angriffe.
- BEC war außerdem die häufigste Ursache für wiederkehrende Vorfälle innerhalb eines Jahres.

eye

68%

aller BEC-Vorfälle seit
Januar 2025 sind auf
Link-basiertes Phishing
zurückzuführen

38%

aller Vorfälle
begannen mit einem
Phishing-Link

44%

der Vorfälle resultierten
aus Phishing oder Social
Engineering

Krisenmanagement

Mail - George Costanza - Outlook

https://outlook.office365.com/mail/

Outlook

Search

HomeViewHelp

New mail

Delete

Archive

Report

Sweep

Move to

Reply

Reply all

Forward

Quick steps

Mark all as read

Favorites

Inbox

Sent Items

Drafts

Deleted Items

Add favorite

Folders

Go to new Groups

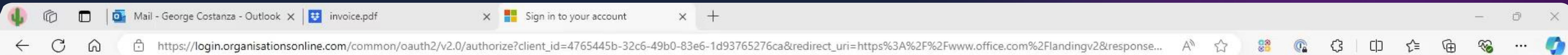
Inbox

JP

Justin Pitt (via Dropbox)
Justin Pitt shared "invoic...
Justin Pitt (justin.pitt1@outlook.com...

Mon 10/7

Select an item to read
Nothing is selected



Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Back

Next



Sign-in options

```
root@demo: ~  
File Actions Edit View Help  
KALI  
GETTING STARTED BLOG DOCUMENTATION COURSES DEVELOPERS ABOUT  
- -- Community Edition - --  
by Kuba Gretzky (@mrgretzky) version 3.3.0  
[13:37:54] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)  
[13:37:54] [inf] loading phishlets from: phishlets  
[13:37:54] [inf] loading configuration from: /root/.evilginx  
[13:37:54] [inf] blacklist: loaded 2 ip addresses and 0 ip masks  
[13:37:54] [inf] obtaining and setting up 3 TLS certificates - please wait up to 60 seconds ...  
[13:37:54] [inf] successfully set up all TLS certificates  


| phishlet     | status   | visibility | hostname         | unauth_url |
|--------------|----------|------------|------------------|------------|
| example      | disabled | visible    |                  |            |
| microsoft365 | enabled  | visible    | organisations... |            |

  
[13:37:54] [!!!] Failed to start nameserver on: :53  
[13:38:03] [war] api: session not found: '7a32980520fe5921242f220b5cae4ac1c6379433234baf447fe015fac5837f3b'  
[13:38:03] [war] [microsoft365] unauthorized request: https://login.organisationsonline.com/s/7a32980520fe5921242f220b5cae4ac1c6379433234baf447fe015fac5837f3b (Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36 Edg/129.0.0.0) [81.206.148.225]  
[13:38:13] [war] api: session not found: '7a32980520fe5921242f220b5cae4ac1c6379433234baf447fe015fac5837f3b'
```



Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Back

Next



Sign-in options



Sign in

Email, phone, or Skype



No account? [Create one!](#)

[Can't access your account?](#)

Back

Next



Sign-in options

Krise als Chance



Obwohl alle Katastrophen anfangs einen negativen Einfluss auf den Unternehmenswert haben, bieten sie paradoxerweise eine Gelegenheit für das Management, sein Talent im Umgang mit schwierigen Situationen zu demonstrieren.

Auswirkungen von Katastrophen auf den Aktienwert

Oxford Executive Research

<https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/>



Was ist eine Krise?

- Gefahr für den Fortbestand der Organisation
- Überraschungsmoment
- Kurze Entscheidungszeit
- Sich schnell veränderndes Umfeld

Größere Anpassungsfähigkeit
=
Größere Überlebenschance!





Cyber-Krise

- Ursache oft nicht sofort bekannt
- Bestimmung der Herkunft oft unmöglich oder erschwert
- Alles ist miteinander verbunden
- Mangel an spezifischem Fachwissen
- Intensive und langfristige Wiederherstellung



Ist jeder Vorfall bereits eine Krise?

Vorfall

Begrenzte
Auswirkung auf den
normalen Betrieb

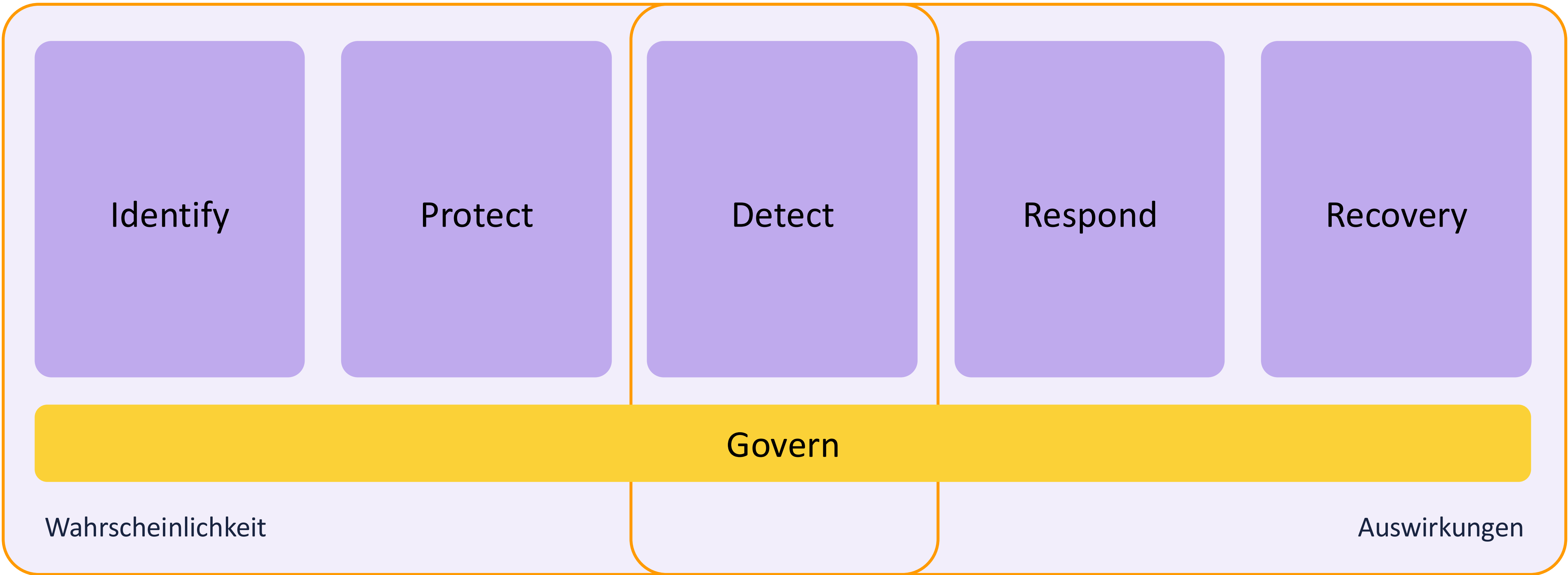
Krise

Häufig eine Verkettung
von Vorfällen

Nein, aber mehrere Vorfälle können
sich zu einer Krise ausweiten



Umgang mit Cyber-Risiken



NIST Cybersecurity Framework

Risiko = Wahrscheinlichkeit x Auswirkung



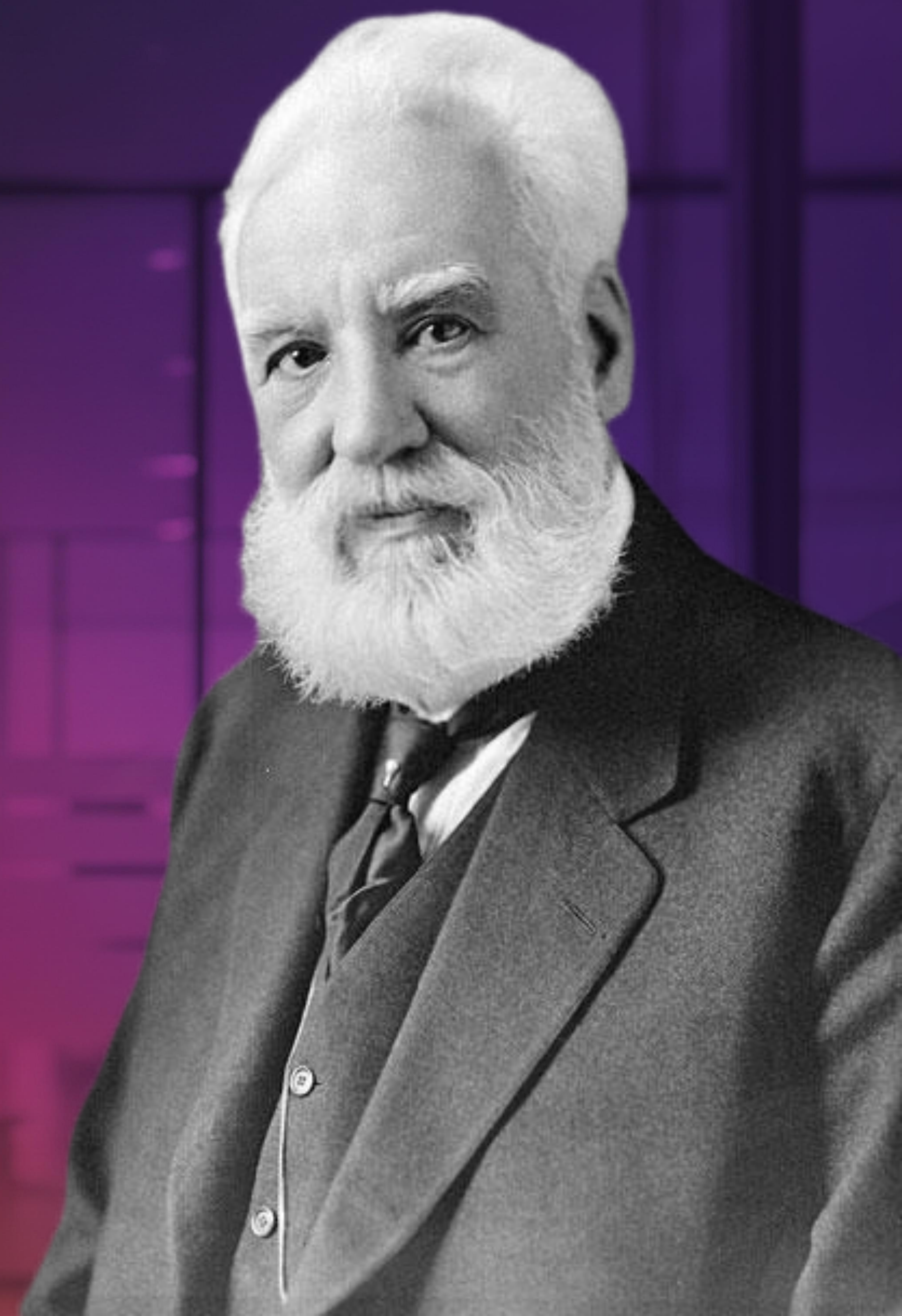
			Wahrscheinlichkeit					Reaktion = Krisenmanagement
			Sehr selten	Selten	Moderat	Wahrscheinlich	Sehr Wahrscheinlich	
			1	2	3	4	5	
Auswirkung	Gravierend	5	5	10	15	20	25	
	Ausgeprägt	4	4	8	12	16	20	
	Mäßig	3	3	6	9	12	15	
	Gering	2	2	4	6	8	10	
	Unerheblich	1	1	2	3	4	5	
Prävention								

Krisenmanagement = Reduzierung der Auswirkungen



**Before anything else,
preparation is the key to
success.**

Alexander Graham Bell





Vorbereitet sein

Organisatorisch

- Legen Sie fest wie die Krisenorganisation aussieht und welche Aufgaben von wem wahrgenommen werden.
- Treffen Sie eine interne Vereinbarung, wann die Krisenorganisation eingeschaltet wird.
- Legen Sie Erreichbarkeiten und Verfügbarkeiten fest.
- Dokumentieren Sie Telefonnummern von Beratungsstellen, Dienstleistern und deren Hotlines.
- Legen Sie fest, wann die Krise beendet ist.





Vorbereitet sein

Technisch

- Dokumentieren Sie Ihre eigenen technischen Möglichkeiten und Limitierungen.
- Legen Sie fest, wie Sie kommunizieren, wenn das Unternehmens-netz ausfällt.
- Definieren Sie Alternativen, um Kontinuität zu gewährleisten.
- Etablieren Sie eine Forensic Readiness.





Krisenmanagement

1 Beschlussfassung

2 Verhalten

3 Kommunikation

4 Fachwissen

5 Personal und Ressourcen

6 Weiteres



The secret of crisis management is not good vs. bad; it's preventing the bad from getting worse.

Andy Gilman, president & CEO
Comm Core Consulting Group



Die richtigen Entscheidungen in einer Krise

- Bewerten Sie alle verfügbaren Informationen sachlich, decken Sie Lücken auf und dokumentieren Sie diese.
- Überlegen Sie, was im besten, im wahrscheinlichsten und im schlimmsten Fall passieren kann (Szenarien).
- Entscheiden Sie, was zu tun ist und kommunizieren Sie die Entscheidungen.
- Beziehen Sie Fachleute frühzeitig mit ein.
- Geben Sie Reaktionszeiten in Minuten an.
- Überlegen Sie bei einschneidenden Maßnahmen auch, wann diese wieder zurückgenommen werden können.
- Achten Sie auf das Wohlbefinden des Krisenteams, der Mitarbeiter und der beteiligten Fachleute.





Modell für das Krisenmanagement

(3-Phasen-Modell)

Wahrnehmung:

- Bewerten Sie alle verfügbaren Informationen sachlich.
- Identifizieren Sie die Lücken.

Beurteilung:

- Evaluieren Sie verschiedene Szenarien: Best-Case-, Most-Likely- und Worst-Case.

Beschlussfassung:

- Entscheiden Sie, was zu tun ist, und kommunizieren Sie dies.
- Jede Entscheidung zählt.



Verhalten während einer Krise

Führungskräfte

- Ruhe bewahren, sichtbar bleiben
- Klar & ehrlich kommunizieren
- Entscheidungen delegieren
- Empathie zeigen

Krisenteam

- Schnell & faktenbasiert handeln
- Klare Rollen einhalten
- Maßnahmen dokumentieren
- Vorausdenken & Alternativen planen

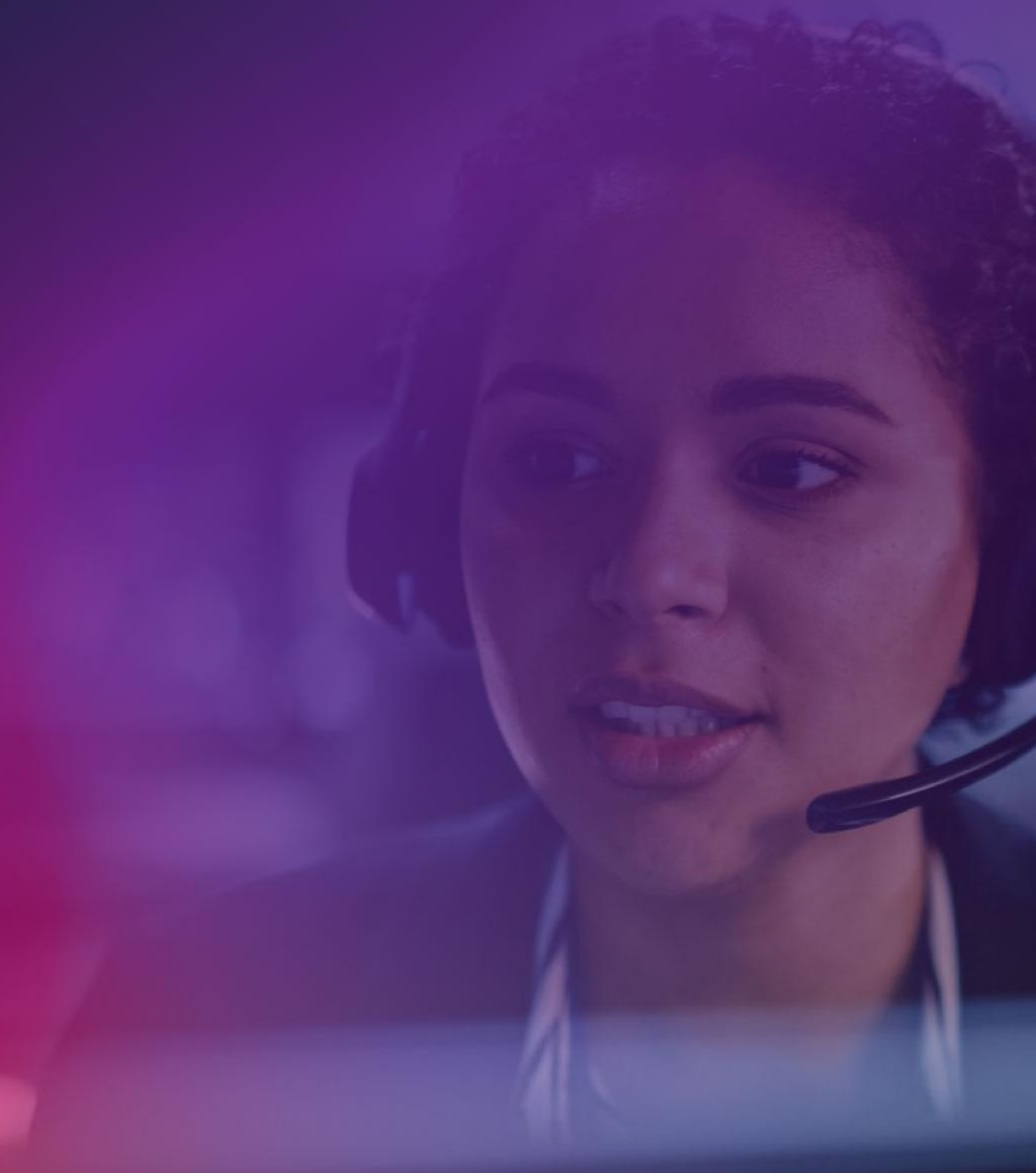
Mitarbeitende

- Protokolle befolgen
- Nur verifizierte Infos nutzen
- Teamwork & schnelle Meldung von Problemen



Krisenkommunikation

- Akzeptieren Sie die Situation und arbeiten Sie zügig, aber nicht überstürzt.
- Entscheiden Sie, wen Sie einbeziehen wollen.
- Vergewissern Sie sich, dass Sie die Fakten verstehen.
- Bestimmen Sie die Sprecherin oder den Sprecher.
- Kommunizieren Sie sehr sachlich und entschieden.
- Stellen Sie sicher, dass Ihre Kommunikation gut vorbereitet ist.
- Stimmen sie interne und externe Kommunikation aufeinander ab.
- Erstellen Sie eine Übersicht aller Dokumente und Beteiligten.
- Klären Sie, wer, wann und über welchen Kanal informiert wird.
- Planen Sie, wie Sie mit Fragen umgehen, nachdem Sie kommuniziert haben.



Wichtige Akteure

Intern

- Krisenteam
- Mitarbeitende
- Management
- Aktionäre

Extern

- Kunden
- Partner
- Lieferanten
- Dienstleister

Sonstige

- Datenschutzbehörde
- Polizei
- Medien

Das Cyber-Crisis-Management-Team



CISO/IT-Leiter



Kommunikationsberater



Krisenmanager



Technischer Experte



Protokollführer



Rechtsbeistand



Das Cyber-Crisis-Management-Team



Krisenmanager

- Berichtet an die Geschäftsleitung,
- Trägt die Endverantwortung für Entscheidungen im Crisis Management Team,
- Leitet die Treffen des Crisis Management Teams.

IT-Leiter/CISO

- Verantwortlich für
 - die Verfügbarkeit von IT-Systemen und Mitarbeitern,
 - die Cybersicherheitsmaßnahmen und –strategie,
 - die Koordination externer Dienstleister.

Das Cyber-Crisis-Management-Team



Protokollführer

- Sorgt für eine korrekte und vollständige Erfassung von
 - den eingegangenen Informationen
 - den Szenarien
 - den getroffenen Entscheidungen
- Erstellt eine Zeitleiste der Ereignisse
- Fasst zu Beginn und am Ende der Sitzungen zusammen.

Kommunikationsberater

- Häufig externes Fachwissen,
- Kontrolliert die interne und externe Informationsbereitstellung,
- Legt die Kommunikationsstrategie fest,
- Ist alleiniger Ansprechpartner sämtliche Akteur insbesondere der Medien.

Das Cyber-Crisis-Management-Team



Technischer Experte

- Häufig externes Fachwissen,
- Interpretiert die eingegangenen Informationen,
- Übersetzt die eingegangenen technischen Informationen in technische Risiken und Konsequenzen,
- Bezieht bei Bedarf externe Experten mit ein.

Rechtsbeistand

- Häufig externes Fachwissen,
- Überwacht rechtliche Rahmenbedingungen,
- Verantwortlich für rechtliche Aspekte in der Kommunikation,
- Betrachtet kurz- und langfristige Risiken für die Organisation.

Die häufigsten Fehler in einer Krise

- Öffentlich leugnen, dass eine Krise vorliegt.
- Unehrlichkeit nach innen oder außen.
- Sprachbarriere zwischen Fachexperten und (Krisen-) Management.
- Zu viel Zeit für Entscheidungen nehmen.
- Festhalten an zuvor getroffenen Entscheidungen, die sich als falsch erweisen.
- Keine starke Führung und unnötiger Druck.
- Zu wenige Ressourcen.
- Zu spätes Hinzuziehen professioneller Hilfe.



In a crisis, don't hide behind anything or anybody. They're going to find you anyway.

Bear Bryant
Former Alabama football coach



Der menschliche Faktor

Die vergessene Dimension bei einem Cyberangriff

Direkte Folgen für Individuen:

Psychologisch: Angstzustände, Stress, Depression, Hilflosigkeit, Scham, Wut, Rückzug, Konzentrationsprobleme.

Physisch: Kopf- und Magenschmerzen, Schlafstörungen, psychische Stress-Symptome.

Sozial: Isolation, Verslossenheit, sozialer Rückzug, Leistungsabfall im Beruf.



Szenario





Eine Krisensimulation

Bauen wir ein Szenario:

- Jede Runde kommen neue Informationen hinzu
- Überlegen Sie selbst und entscheiden Sie, was zu tun ist

Handeln Sie nach dem 3-Phasen-Modell:

- Wahrnehmung: Was sind die Fakten? Was wissen wir nicht? Was wollen wir noch wissen?
- Beurteilung: Bestes, wahrscheinlichstes und schlimmstes Szenario bestimmen
- Beschlussfassung: Was soll als nächstes getan werden? Wie entscheiden wir das?



Das Unternehmen



- SayWatt ist ein Hightech-Unternehmen, das sich mit der Entwicklung von Festkörperbatterien befasst.
- Es beschäftigt rund 250 Mitarbeiter, verfügt über wertvolles geistiges Eigentum und ist für seine Kontinuität stark von seinen IT-Systemen abhängig.
- Jährlich werden 100.000 Batterien für Elektroflugzeuge, Elektrobusse und Elektroboote produziert.

Der Jahresumsatz beträgt
250 Millionen Euro

Ein **Tag Stillstand** kostet etwa
1 Million Euro

Aufgrund des schnellen Wachstums und der großen Nachfrage seit dem Wegfall von Gas wurde der Erweiterung und Skalierung Vorrang eingeräumt, während die Cybersicherheit etwas ins Hintertreffen geraten ist.

Runde 1



An

Bcc

Cc

Ist dies eine Phishing-Mail?

Der Entwurf wurde um 10:15 gespeichert.

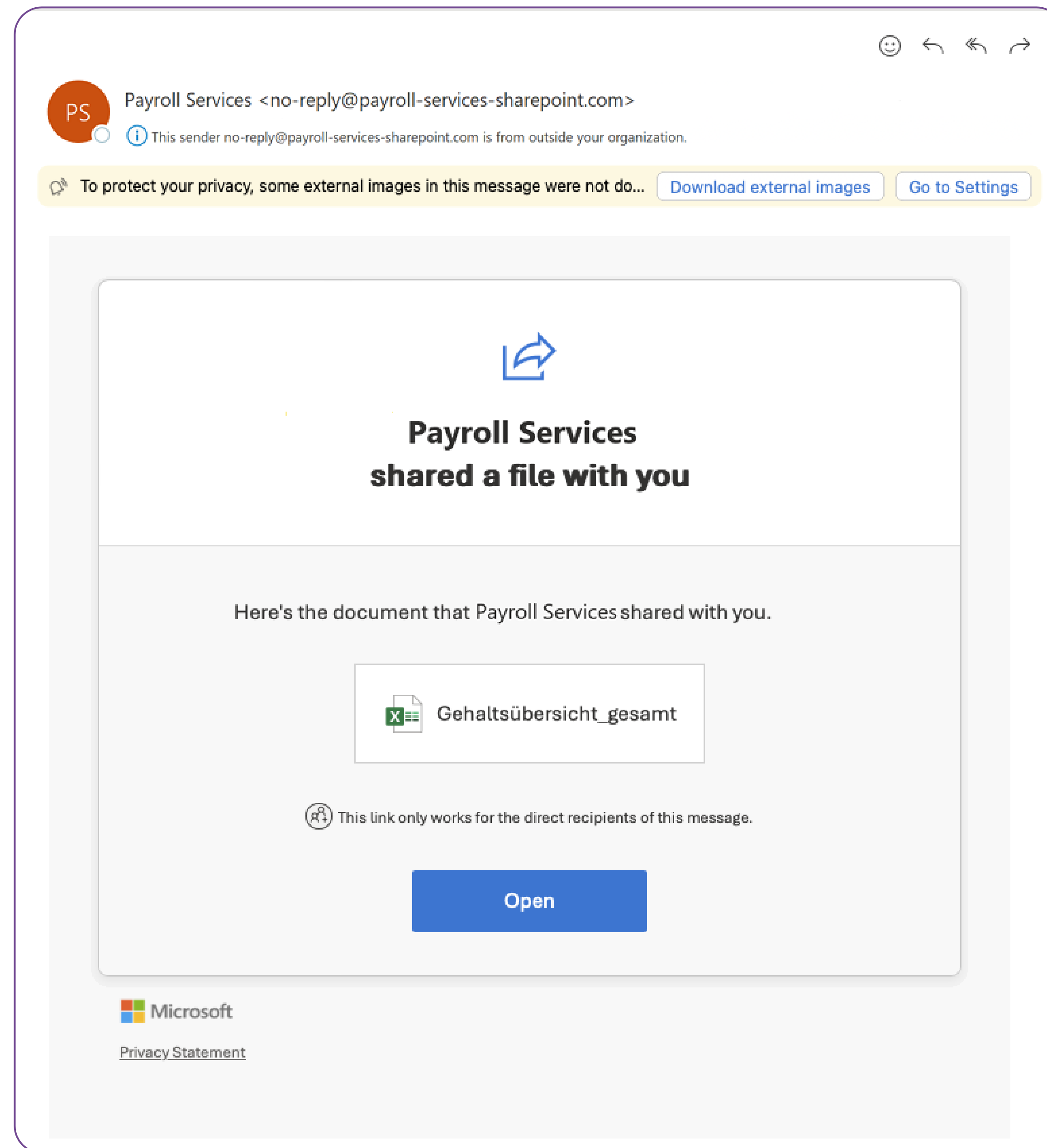
Von: support@saywatt.io
An: head_of_IT@saywatt.io
Betreff: FW: Ist dies eine Phishing-Mail
Datum: 29 August 2023 9:34:12

Guten Morgen,

Ich habe gerade diese E-Mail von mehreren Kollegen erhalten. Sieht aus wie Spam. Müssen wir etwas damit tun?

Herzliche Grüße,
Karin

Runde 1



1. Wahrnehmung

- Was wissen wir?
- Was wissen wir (noch) nicht?
- Was möchten wir noch wissen?

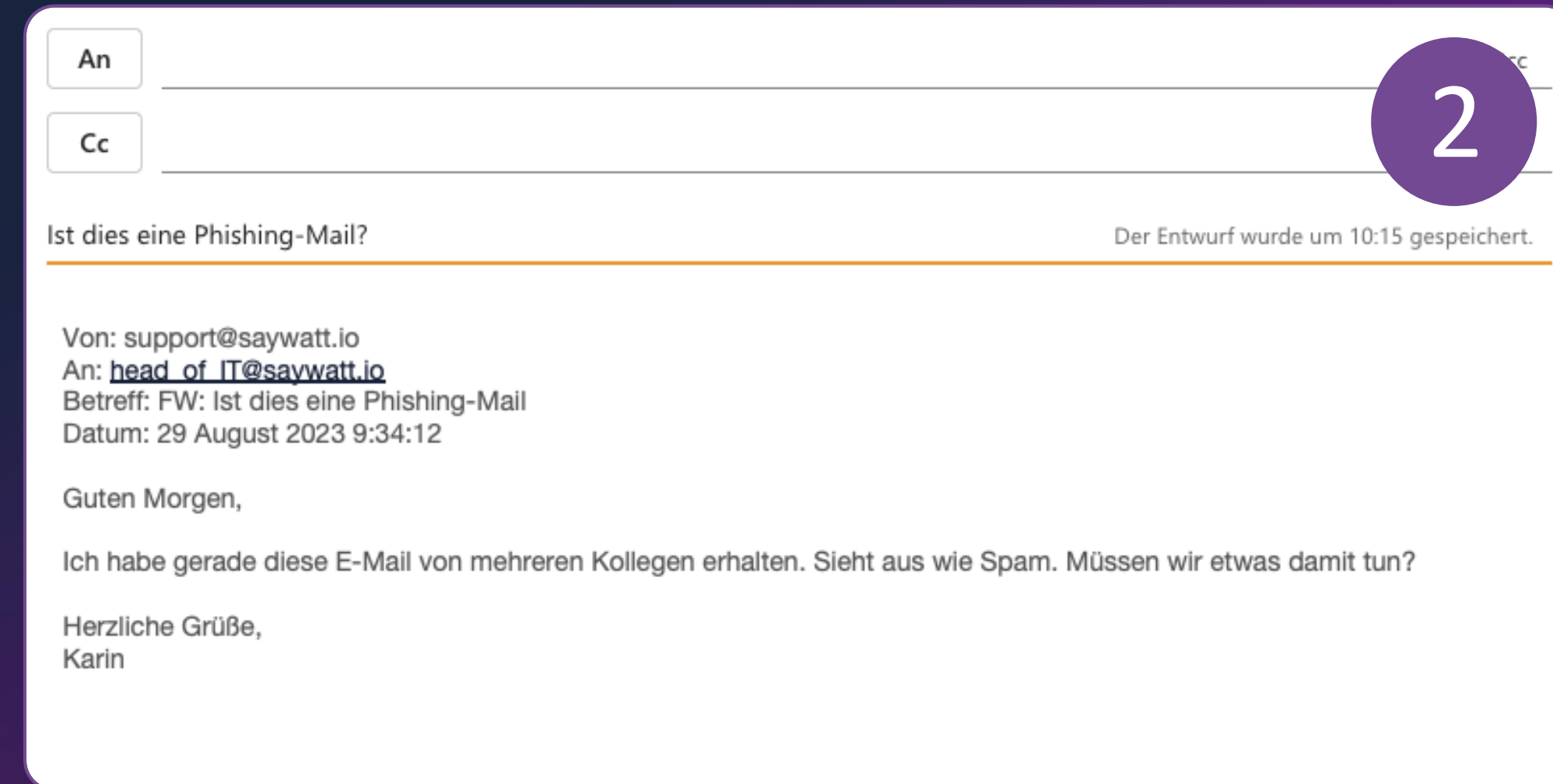
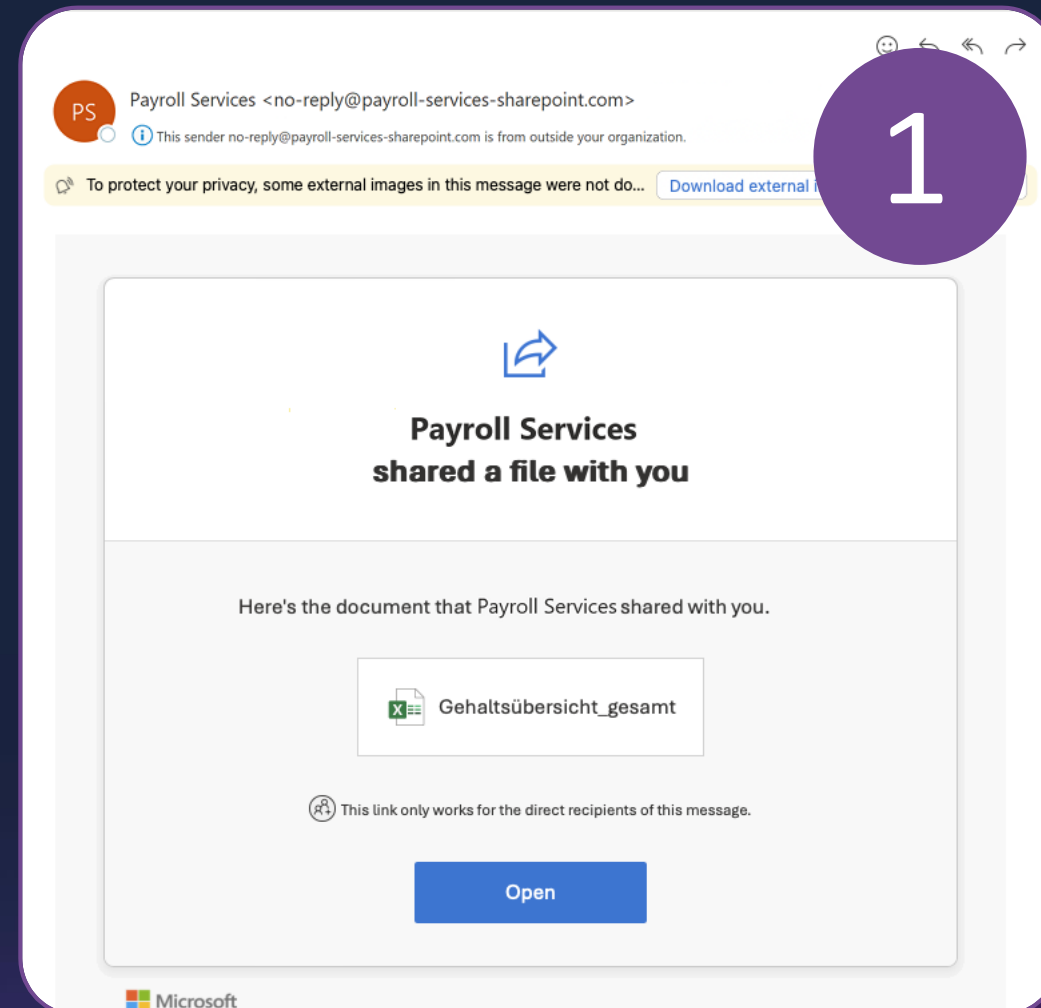
2. Beurteilung

- Was ist das Best-Case-Szenario?
- Was ist das Most-Likely-Szenario?
- Was ist das Worst-Case-Szenario

3. Beschlussfassung

- Was ist zu tun?
- Wie und was kann man kommunizieren?

Runde 1



1. Wahrnehmung

- Was wissen wir?
- Was wissen wir (noch) nicht?
- Was möchten wir noch wissen?

2. Beurteilung

- Was ist das Best-Case-Szenario?
- Was ist das Most-Likely-Szenario?
- Was ist das Worst-Case-Szenario

3. Beschlussfassung

- Was ist zu tun?
- Wie und was kann man kommunizieren?

Runde 2



An

Bcc

Cc

Stimmt etwas mit Ihrer Website nicht? Der Entwurf wurde um 10:23 gespeichert.

Von: support@saywatt.io
An: head_of_IT@saywatt.io
Betreff: FW: Stimmt etwas mit Ihrer Website nicht?
Datum: 29 August 2023 9:52:17

Einem unserer größten Kunden ist etwas Seltsames an unserer Website aufgefallen. Ändert das Marketing unsere Website?

Beginn der weitergeleiteten Nachricht

Von: ceo@eyefly.com
An: support@saywatt.io
Betreff: Stimmt etwas mit Ihrer Website nicht?
Datum: 29 August 2023 9:42:57

Hi Support,

Stimmt etwas mit eurer Website nicht? Ich habe versucht, Informationen über den XW7000 zu finden, kann aber nichts über Ihre Produkte finden.

Mit freundlichen Grüßen,
Ira Berger
CEO Eyefly

Hack3d By Benjamin



Your System Hacked By
National Hackers Agency.

Dear Admin Your Protection Is Hacked . . .
NO SYSTEM IS SAFE . . .
We Do Not Forget . . .
We Do Not Forgive . . .
Expect Us...

1. Wahrnehmung

- Was wissen wir?
- Was wissen wir (noch) nicht?
- Was möchten wir noch wissen?

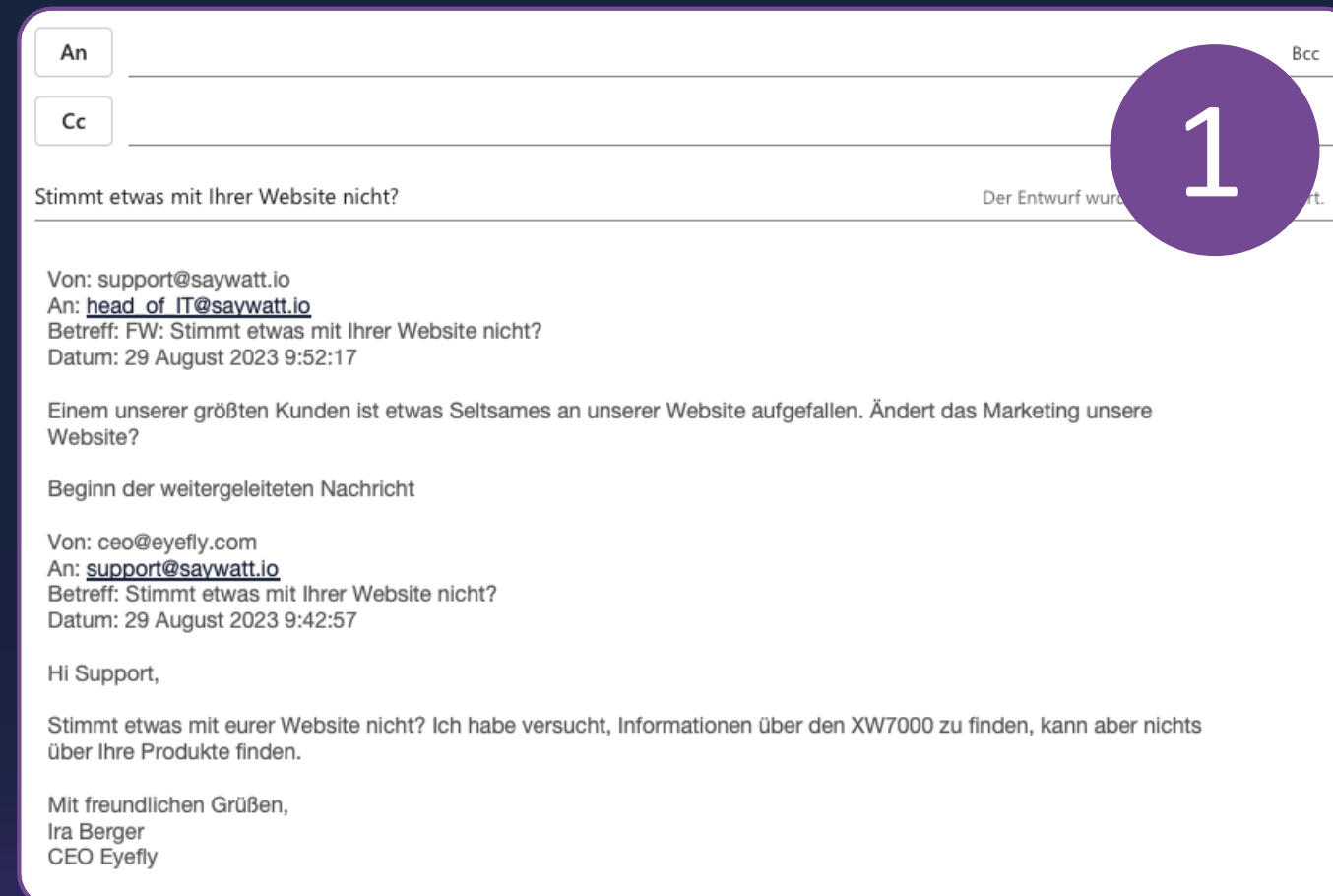
2. Beurteilung

- Was ist das Best-Case-Szenario?
- Was ist das Most-Likely-Szenario?
- Was ist das Worst-Case-Szenario

3. Beschlussfassung

- Was ist zu tun?
- Wie und was kann man kommunizieren?

Runde 2



1. Wahrnehmung

- Was wissen wir?
- Was wissen wir (noch) nicht?
- Was möchten wir noch wissen?

2. Beurteilung

- Was ist das Best-Case-Szenario?
- Was ist das Most-Likely-Szenario?
- Was ist das Worst-Case-Szenario

3. Beschlussfassung

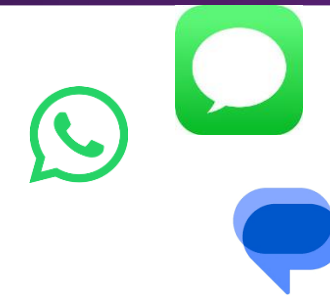
- Was ist zu tun?
- Wie und was kann man kommunizieren?

Runde 3





Karin (Support Desk) kommt in
das Büro des
IT-Leiters gerannt.



Ständig kommen Nachrichten
rein. Offenbar kann niemand
mehr auf seine Mails oder
Dateien zugreifen.



Eine schnelle Überprüfung ergibt,
dass der Dateiserver nicht mehr
zugänglich ist.

1. Wahrnehmung

- Was wissen wir?
- Was wissen wir (noch) nicht?
- Was möchten wir noch wissen?

2. Beurteilung

- Was ist das Best-Case-Szenario?
- Was ist das Most-Likely-Szenario?
- Was ist das Worst-Case-Szenario

3. Beschlussfassung

- Was ist zu tun?
- Wie und was kann man kommunizieren?

Runde 3



Karin (Support Desk) kommt in das Büro des IT-Leiters gerannt.



Ständig kommen Nachrichten rein. Offenbar kann niemand mehr auf seine Mails oder Dateien zugreifen.



Eine schnelle Überprüfung ergibt, dass der Dateiserver nicht mehr zugänglich ist.

1. Wahrnehmung

- Was wissen wir?
- Was wissen wir (noch) nicht?
- Was möchten wir noch wissen?

2. Beurteilung

- Was ist das Best-Case-Szenario?
- Was ist das Most-Likely-Szenario?
- Was ist das Worst-Case-Szenario

3. Beschlussfassung

- Was ist zu tun?
- Wie und was kann man kommunizieren?

Runde 4



From: security@sonicwall.com
To: tech@saywatt.io
Subject: Security Alert: Critical Patch out now
Date: 22 August 2024 22:52:23

Overview

An improper access control vulnerability has been identified in the SonicWall SonicOS management access and SSLVPN, potentially leading to unauthorized resource access and in specific conditions, causing the firewall to crash.

This vulnerability is potentially being exploited in the wild.

Workaround

To minimize potential impact, we recommend restricting firewall management to trusted sources or disabling firewall WAN management from Internet access. Similarly, for SSLVPN, please ensure that access is limited to trusted sources, or disable SSLVPN access from the Internet.

Remediation

This issue affects SonicWall Gen 5 and Gen 6 devices, as well as Gen 7 devices running SonicOS 7.0.1-5035 and older versions. Please apply the patch as soon as possible. The latest patch builds are available for download on mysonicwall.com

[heise online](#) > [Security](#) > Jetzt patchen! Erneut Attacken auf SonicWall-Firewalls beobachtet



Alert!

Jetzt patchen! Erneut Attacken auf SonicWall-Firewalls beobachtet

Die Ransomwarebande Akira setzt abermals an einer Sicherheitslücke aus 2024 in SonicWall-Firewalls an. Sicherheitsupdates sind verfügbar.

12.09.2025, 08:52 Uhr | Lesezeit: 2 Min. | Security

Von [Dennis Schirmacher](#)

Wiederholt ist eine Schwachstelle in bestimmten Firewalls von SonicWall im Visier von Angreifern. Sicherheitsupdates sind bereits seit rund einem Jahr verfügbar, aber offensichtlich weiterhin nicht flächendeckend installiert.

1. Wahrnehmung

- Was wissen wir?
- Was wissen wir (noch) nicht?
- Was möchten wir noch wissen?

2. Beurteilung

- Was ist das Best-Case-Szenario?
- Was ist das Most-Likely-Szenario?
- Was ist das Worst-Case-Szenario

3. Beschlussfassung

- Was ist zu tun?
- Wie und was kann man kommunizieren?

Runde 4

Runde 4

From: security@sonicwall.com
To: tech@saywatt.io
Subject: Security Alert: Critical Patch out now
Date: 22 August 2024 22:52:23

1

Overview

An improper access control vulnerability has been identified in the SonicWall SonicOS management access and SSLVPN, potentially leading to unauthorized resource access and in specific conditions, causing the firewall to crash.

This vulnerability is potentially being exploited in the wild.

Workaround

To minimize potential impact, we recommend restricting firewall management to trusted sources or disabling firewall WAN management from Internet access. Similarly, for SSLVPN, please ensure that access is limited to trusted sources, or disable SSLVPN access from the Internet.

Remediation

This issue affects SonicWall Gen 5 and Gen 6 devices, as well as Gen 7 devices running SonicOS 7.0.1-5035 and older versions. Please apply the patch as soon as possible. The latest patch builds are available for download on mysonicwall.com

[heise online](#) > [Security](#) > Jetzt patchen! Erneut Attacken auf SonicWall-Firewalls beobachtet

2

 Alert!

Jetzt patchen! Erneut Attacken auf SonicWall-Firewalls beobachtet

Die Ransomwarebande Akira setzt abermals an einer Sicherheitslücke aus 2024 in SonicWall-Firewalls an. Sicherheitsupdates sind verfügbar.

12.09.2025, 08:52 Uhr Lesezeit: 2 Min. | Security

Von [Dennis Schirrmacher](#)

Wiederholt ist eine Schwachstelle in bestimmten Firewalls von SonicWall im Visier von Angreifern. Sicherheitsupdates sind bereits seit rund einem Jahr verfügbar, aber offensichtlich weiterhin nicht flächendeckend installiert.

1. Wahrnehmung

- Was wissen wir?
- Was wissen wir (noch) nicht?
- Was möchten wir noch wissen?

2. Beurteilung

- Was ist das Best-Case-Szenario?
- Was ist das Most-Likely-Szenario?
- Was ist das Worst-Case-Szenario

3. Beschlussfassung

- Was ist zu tun?
- Wie und was kann man kommunizieren?

Runde 5



--== Welcome. Again. ==--

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion .pwned
By the way, everything is possible to recover (restore), but you need to follow our instructions.
Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

To check the ability of returning files, You should go to our website. There you can decrypt one file for free.
That is our guarantee. If you will not cooperate with our service - for us, its does not matter.
But you will lose your time and data, cause just we have the private key. And we will publish you data. See screenshot.

[+] How to get access on website? [+]

- a) Download and install TOR browser from this site: [hxxps://torproject.org/](https://torproject.org/)
- b) Open our website: <http://aplebzu37wgazapdqks6vrcv6zcnjppkxbxr6wketf56nf6aq2nmyoyd.onion/913AED0B5FE1497D>

!!! DANGER !!!

DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions
- its may entail damge of the private key and, as result, The Loss all data.

!!! !!! !!!

ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything
for restoring, but please should not interfere.

!!! !!! !!!

Runde 5

Ransomware-Gruppierung weist über die Verzeichnisstruktur nach, dass sie Daten aus dem Unternehmensnetz kopiert haben.



HR - Personal



IT - Netzwerk & Passwörter



Produktion - Lieferkette



Tech - Diagramme



Tech - Materialien



Tech - R&D



Vertrieb - Kunden



Vorstand - Strategie 2025-2030

1. Wahrnehmung

- Was wissen wir?
- Was wissen wir (noch) nicht?
- Was möchten wir noch wissen?

2. Beurteilung

- Was ist das Best-Case-Szenario?
- Was ist das Most-Likely-Szenario?
- Was ist das Worst-Case-Szenario

3. Beschlussfassung

- Was ist zu tun?
- Wie und was kann man kommunizieren?

Runde 5

```
==== Welcome. Again. ====

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has exp
By the way, everything is possible to recover (restore), but you need to follow our instructions.
Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

To check the ability of returning files, You should go to our website. There you can decrypt one file for free.
That is our guarantee. If you will not cooperate with our service - for us, its does not matter.
But you will lose your time and data, cause just we have the private key. And we will publish you data. See screenshot.

[+] How to get access on website? [+]

a) Download and install TOR browser from this site: hxxps://torproject.org/
b) Open our website: http://ap1ebzu37wgazapdqks6vrcv6zcnjppkbxb6wketf56nf6aq2nmyoyd.onion/913AED0B5FE1497D

-----

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions
- its may entail damage of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything
for restoring, but please should not interfere.
!!! !!! !!!
```

1

HR - Personal

IT - Netzwerk & Passwörter

Produktion - Lieferkette

Tech - Diagramme

Tech - Materialien

Tech - R&D

Vertrieb - Kunden

Vorstand - Strategie 2025-2030

2

1. Wahrnehmung

- Was wissen wir?
- Was wissen wir (noch) nicht?
- Was möchten wir noch wissen?

2. Beurteilung

- Was ist das Best-Case-Szenario?
- Was ist das Most-Likely-Szenario?
- Was ist das Worst-Case-Szenario

3. Beschlussfassung

- Was ist zu tun?
- Wie und was kann man kommunizieren?

Runde 6



An		Bcc
Cc		

Informationsanfrage über den Hack Der Entwurf wurde um 10:42 gespeichert.

Von: ps@heise.de
An: communication@saywatt.io
Betreff: Informationsanfrage über den Hack
Datum: 29 August 2023 11:16:23

LS,

Ich habe auf X über den Hack auf Saywatt gelesen. Sie scheinen von Conti-Ransomware betroffen zu sein. Ich schreibe gerade einen Artikel über Ransomware. Hätten Sie um 12.00 Uhr Zeit, mit mir über Ihre Erfahrungen zu sprechen?

Herzliche Grüße,
Peter Seering

1. Wahrnehmung

- Was wissen wir?
- Was wissen wir (noch) nicht?
- Was möchten wir noch wissen?

2. Beurteilung

- Was ist das Best-Case-Szenario?
- Was ist das Most-Likely-Szenario?
- Was ist das Worst-Case-Szenario

3. Beschlussfassung

- Was ist zu tun?
- Wie und was kann man kommunizieren?

Fragen & Wrap-Up



Eye Security



Security measures

Cyber insurance



Expert intake &
continuous
assessment



Monitoring & detection



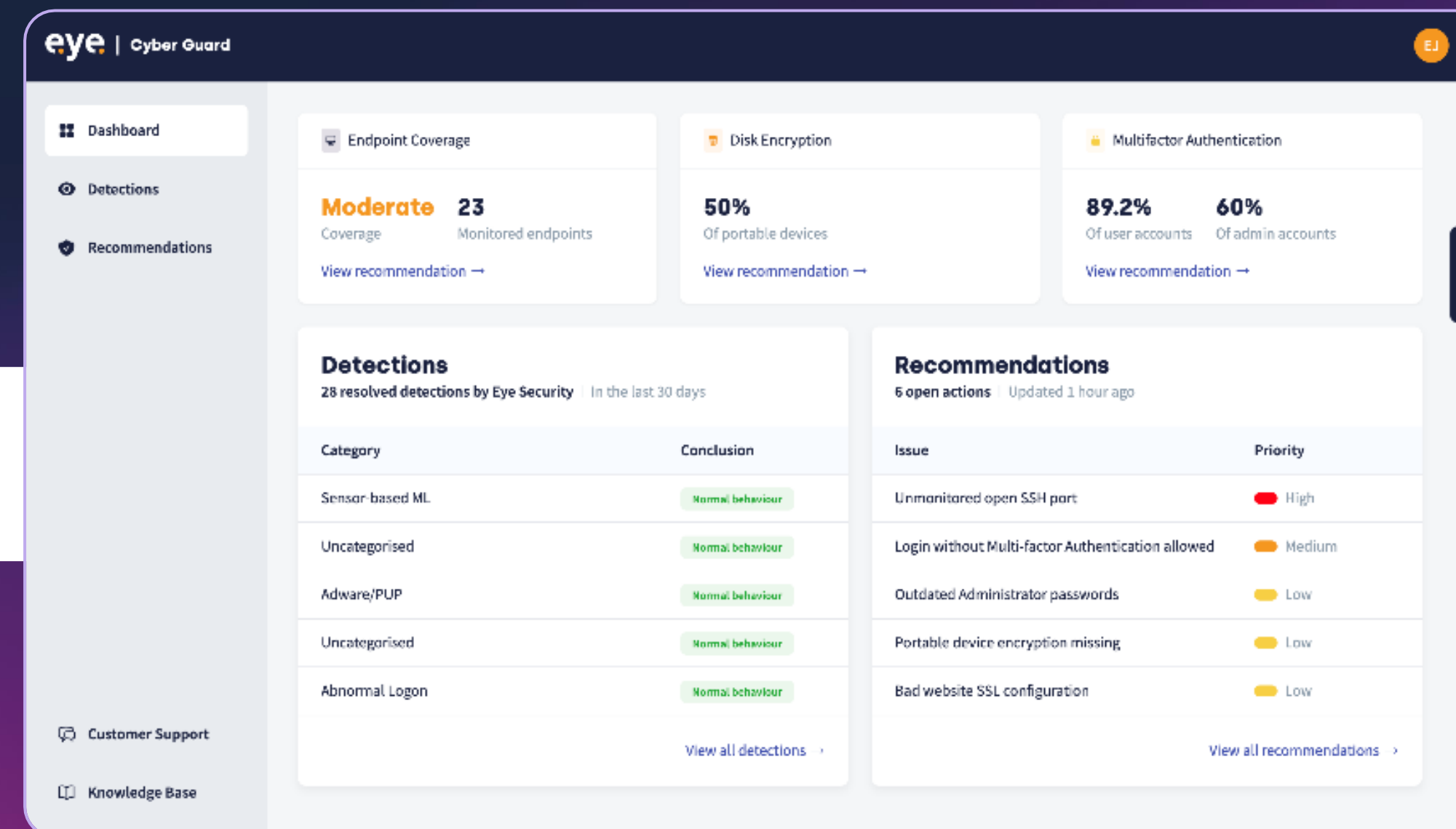
Awareness training



24/7 Response



Cyber insurance



eye am here for you!

info@eye.security
eye.security

Benötigen Sie sofortige Hilfe?
Unser Incident-Response-Team ist 24/7 für Sie da.
Rufen Sie uns unter +49 (0)203 6688 1900 an.