oneconsult
together against cyberattacks

Fit werden für den Cybervorfall

Tabea Nordieker | Nürnberg, 23. Oktober 2024

Tabea Nordieker

Senior Digital Forensics & Incident Response Specialist

MSc UNIL Digital Forensics, GCFA, GCFR, BTL1

T: +41 43 377 22 46

E: tabea.nordieker@oneconsult.com

Übung macht den Meister

https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

OVERVIEW

An Incident Response Plan is a written document, formally approved by the senior leadership team, that helps your organization *before*, *during*, and *after* a confirmed or suspected security incident. Your IRP will clarify roles and responsibilities and will provide guidance on key activities. It should also include a cybersecurity list of key people who may be needed during a crisis.

BEFORE A CYBERSECURITY INCIDENT

- **Conduct an attack simulation exercise**, sometimes called a tabletop exercise, or TTX. A TTX is a role-playing game where a facilitator presents a scenario to the team. The exercise might start with the head of communications receiving an email from a reporter about rumors of a hack. The facilitator will provide other updates during the game to see how everyone plays their role. Every sports team rehearses, and you should too!

Trainingsplan erstellen

Was soll trainiert werden

Vorbereitung und Durchführung

Was wäre wenn…

Foto von Dave Photoz auf Unsplash

Alle Dateien sind verschlüsselt

Hello!

If you are reading this, it means that your system were hit by Royal ransomware.
Please contact us via :
http://royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid.onion/[snip]

In the meantime, let us explain this case.It may seem complicated, but it is not!
Most likely what happened was that you decided to save some money on your security infrastructure.
Alas, as a result your critical data was not only encrypted but also copied from your systems on a secure server.
From there it can be published online.Then anyone on the internet from darknet criminals, ACLU journalists, Chinese government(different names for the sam
and even your employees will be able to see your internal documentation: personal data, HR reviews, internal lawsuitsand complains, financial reports, accou

Fortunately we got you covered!

Royal offers you a unique deal.For a modest royalty(got it; got it ?) for our pentesting services we will not only provide you with an amazing risk mitigation se
covering you from reputational, legal, financial, regulatory, and insurance risks, but will also provide you with a security review for your systems.
To put it simply, your files will be decrypted, your data restoredand kept confidential, and your systems will remain secure.

Try Royal today and enter the new era of data security!
We are looking to hearing from you soon!

Eine Schwachstelle wird veröffentlicht

VMWARE | ESXI

CVE-2024-37085

VMware ESXi Authentication Bypass Vulnerability: *VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD.*

Known To Be Used in Ransomware Campaigns? **Known**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-07-30
- **Due Date:** 2024-08-20

Additional Notes +

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Kompromittierung eines Microsoft 365 Accounts

From: [redacted]
Sent on: Wednesday, January 17, 2024 11:19:01 AM
To: Undisclosed recipients:;
Subject: Angebot Nr. 2735322 Installationen

[redacted] shared a folder with you

Here's the folder that [redacted] shared with you.

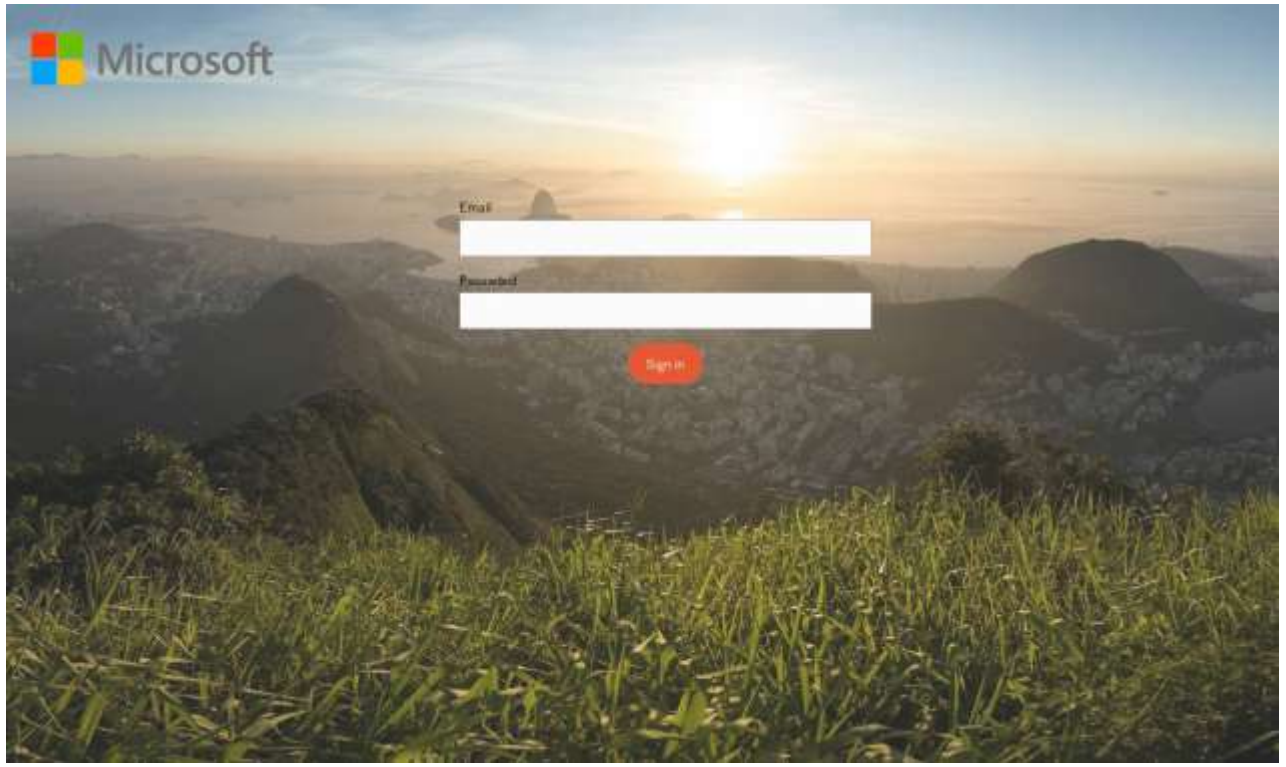
[redacted]

This link only works for the direct recipients of this message.

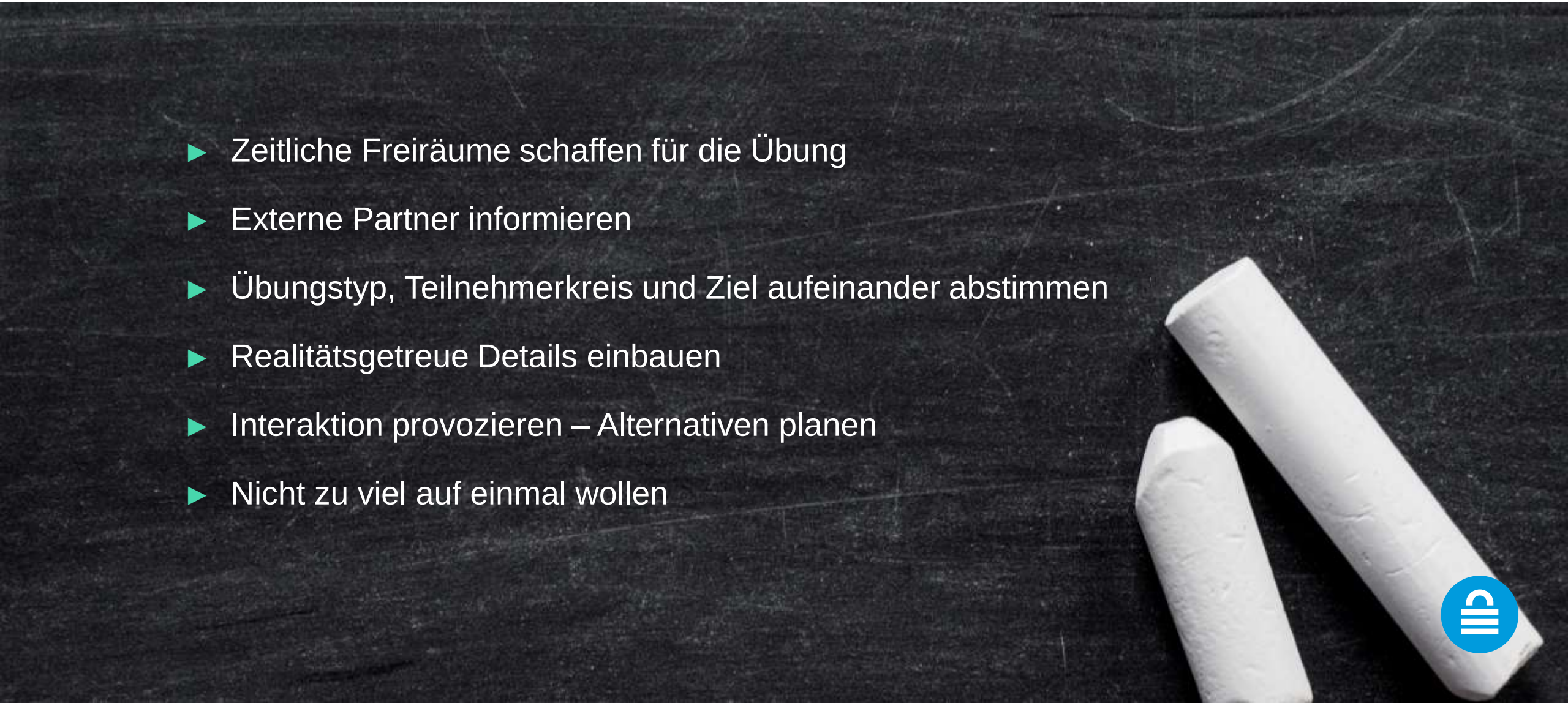
Open

Microsoft Privacy Statement

Freundliche Grüsse
[redacted]



Lessons Learned



- Zeitliche Freiräume schaffen für die Übung
- Externe Partner informieren
- Übungstyp, Teilnehmerkreis und Ziel aufeinander abstimmen
- Realitätsgetreue Details einbauen
- Interaktion provozieren – Alternativen planen
- Nicht zu viel auf einmal wollen

Lassen Sie sich von Vorfällen inspirieren:
Was würde in Ihrer Organisation geschehen?

Photo by Clint Bustrillos on Unsplash

Wollen Sie mehr erfahren?

Blogartikel

Tabletop-Übungen: Ihr Krisenmanagement auf dem Prüfstand

Let's connect

www.oneconsult.com

/oneconsult-ag

/OneconsultAG

/oneconsult

Monatliche Cybersecurity News abonnieren:

Oneconsult Newsletter