TECHNISCHE HOCHSCHULE DEGGENDORF

WIE SICHER IST IHR UNTERNEHMEN?

LEGALES HACKEN FÜR EINE SICHERE ZUKUNFT

Campus Vilshofen | Cybersecurity

www.th-deg.de/tc-vilshofen

Campus Vilshofen

CYBERSECURITY

KEY FACTS
ZUM FORSCHUNGSSTANDORT

Informationstechnologie begleitet uns beinahe überall: von Mobiltelefonen, PKWs und Smart-Home-Produkten über Onlineanwendungen im Finanz- oder Gesundheitswesen bis hin zu personalisierter Werbung.

Sicher haben auch Sie sowohl privat als auch in Ihrem Unternehmen sehr viele Schnittpunkte im Bereich IT.

In jeder Branche und Unternehmensgröße schreitet die Digitalisierung voran: Prozesse werden automatisiert und Systeme miteinander verbunden. Kritische Geschäftsanwendungen erfolgen immer häufiger webbasiert und stetig werden mehr Anwendungen und Daten in die Cloud verlagert.

Oft unterschätzt man die daraus resultierenden Gefahren und die Notwendigkeit, die Cybersicherheit gleichermaßen zu stärken.

Vor allem die rasante Weiterentwicklung im Bereich Künstliche Intelligenz – darunter fortschrittliche Technologien wie GenAI (generative KI) – führt zur kontinuierlichen Professionalisierung von Cyberangriffen.

Trotzdem reichen oft einfache Maßnahmen, um ein Unternehmen besser zu schützen – und das auch mit geringen eigenen Ressourcen. Als kompetenter Ansprechpartner mit Expertise aus Forschung und Anwendung unterstützen wir Sie dabei, das Sicherheitsniveau Ihres Unternehmens zu evaluieren und zu optimieren.

Dazu bieten wir Ihnen Sicherheitsprüfungen und -maßnahmen sowie Schulungen und Mitarbeitendentrainings, die auf Ihr Unternehmen und Ihre Bedarfe zugeschnitten sind.

Auf den folgenden Seiten möchten wir Ihnen einen Auszug unseres Serviceangebots vorstellen.

Ihr Team des Campus Vilshofen

INHALT

VORWORT	03
PENETRATIONSTESTS	06 – 07
PENTEST: ASSUMED BREACH	08 – 09
PENTEST: ACTIVE DIRECTORY	10 – 11
SMB-FREIGABENCHECK	12 – 13
STOLEN-DEVICE-CHECK	14 – 15
PASSWORTAUDIT	16 – 17
WEBANWENDUNGS- & SOFTWARECHECK	18 – 19
PHISHINGSIMULATION	20 – 21
SICHERN SIE IHR UNTERNEHMEN	22 – 23

Ar_TH | stock.adobe.com


LIVE CYBER THREAT MAP
CHECK POINT
Malware
Phishing
Exploit
Australia

PENETRATIONSTESTS
SICHERHEITSPRÜFUNG

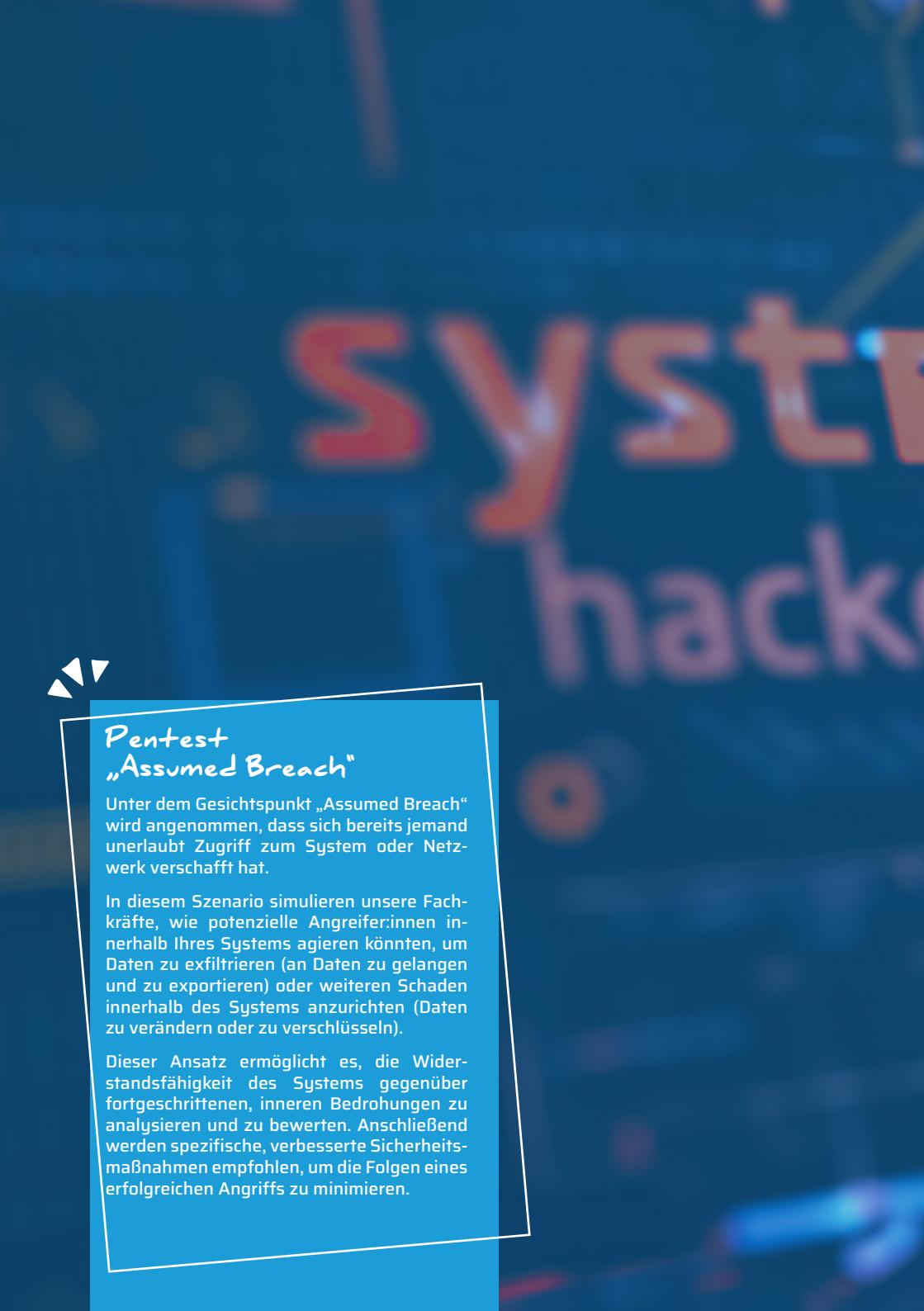
Ein Pentest (kurz für Penetrationstest) ist eine gezielte Sicherheitsprüfung, bei der unsere Expert:innen Schwachstellen in einem Computersystem, Netzwerk oder einer Anwendung aufdecken und je nach Vereinbarung auch ausnutzen. Ziel ist es, Sicherheitslücken zu finden, bevor potenzielle Angreifer:innen dies tun können.

Pentests gibt es in verschiedenen Ausprägungen. Diese können beispielsweise ein einzelnes System, eine bestimmte (Web-)Anwendung oder einen größeren Umfang an Systemen umfassen.

Generell wird zwischen Tests einer internen oder externen Infrastruktur unterschieden. Beim Pentest einer internen Infrastruktur können zusätzliche Aspekte untersucht werden, beispielsweise SMB-Freigaben oder das Active Directory.

Sicherheitslücken erkennen,

BEVOR SIE AUSGENUTZT WERDEN.



Pentest „Assumed Breach"

Unter dem Gesichtspunkt „Assumed Breach" wird angenommen, dass sich bereits jemand unerlaubt Zugriff zum System oder Netzwerk verschafft hat.

In diesem Szenario simulieren unsere Fachkräfte, wie potenzielle Angreifer:innen innerhalb Ihres Systems agieren könnten, um Daten zu exfiltrieren (an Daten zu gelangen und zu exportieren) oder weiteren Schaden innerhalb des Systems anzurichten (Daten zu verändern oder zu verschlüsseln).

Dieser Ansatz ermöglicht es, die Widerstandsfähigkeit des Systems gegenüber fortgeschrittenen, inneren Bedrohungen zu analysieren und zu bewerten. Anschließend werden spezifische, verbesserte Sicherheitsmaßnahmen empfohlen, um die Folgen eines erfolgreichen Angriffs zu minimieren.

Viks_jin | stock.adobe.com

ACTIVE DIRECTORY
IM FOKUS DER SICHERHEIT

Das Active Directory ist der zentrale Ort für alle Identitäten (Benutzer, Computer, Clients, Gruppen, Drucker etc.) im Unternehmensnetzwerk.

In einer Prüfung des Active Directory identifizieren unsere Sicherheitsexpert:innen Schwachstellen und potenzielle Angriffsvektoren. Dazu werden verschiedene Szenarien simuliert, die unter anderem die (Windows-)Konfiguration, Berechtigungen oder Sicherheitsrichtlinien betreffen.

Ziel ist es, Ihrem Unternehmen Empfehlungen zur Verbesserung Ihrer Sicherheitsmaßnahmen und -richtlinien zu geben, um unautorisierten Zugriff und mögliche Kompromittierungen zu verhindern.

Angriffsvektoren identifizieren

UND SICHERHEITSRICHTLINIEN OPTIMIEREN.

SMB-FREIGABENCHECK
SCHUTZ SENSIBLER DATEN

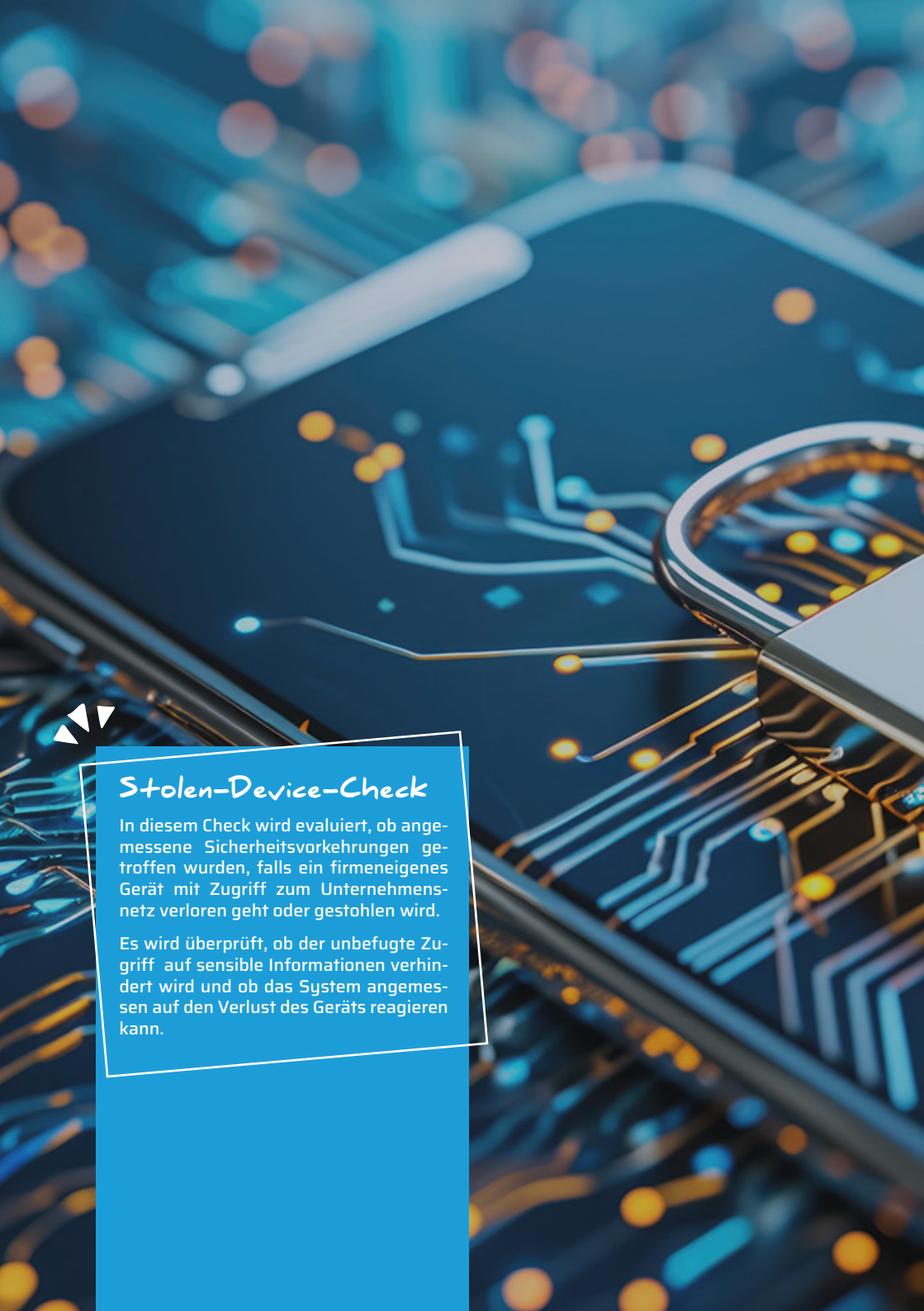
SMB-Freigaben ermöglichen den Zugriff und das Teilen von Dateien und Diensten innerhalb eines lokalen Netzwerks. Dadurch können Benutzerkonten auf ein gemeinsames Laufwerk oder verschiedene Programme auf einen Drucker zugreifen. Oft werden jedoch potenziell vertrauliche oder sensible Informationen unreguliert abgelegt.

Ein SMB-Freigabencheck beinhaltet unter anderem die Suche nach sensiblen Daten und eine Analyse der dazugehörigen Zugriffsberechtigungen. Desweiteren wird evaluiert, ob unangemessene Zugriffsrechte vorliegen und ob diese Angreifer:innen ermöglichen, auf sensible Daten zuzugreifen.

Der Test zielt darauf ab, Schwächen in der Zugriffskontrolle und Datensicherheit aufzudecken und dem Unternehmen entsprechende Empfehlungen zu geben.

Zugriffskontrollen prüfen
UND DATENLECKS VERHINDERN.

ImageFlow | stock.adobe.com



Stolen-Device-Check

In diesem Check wird evaluiert, ob angemessene Sicherheitsvorkehrungen getroffen wurden, falls ein firmeneigenes Gerät mit Zugriff zum Unternehmensnetz verloren geht oder gestohlen wird.

Es wird überprüft, ob der unbefugte Zugriff auf sensible Informationen verhindert wird und ob das System angemessen auf den Verlust des Geräts reagieren kann.

TOP TEN
PASSWÖRTER

01
123456

02
password

03
12345

04
12345678

05
abc123

06
123456789

07
1234567

08
qwerty

09
iloveyou

10
password1

Laut Pressemitteilung der Universität Bonn: *„123456" bleibt das beliebteste Passwort der Deutschen"* vom 29.11.2024.

PASSWORTAUDIT
PASST ODER PASST NICHT?

Ein Passwortaudit bietet wertvolle Einblicke in die Passwortsicherheit eines Unternehmens. Dabei werden die Hashes aller Benutzerkonten im Active Directory (zentraler Ort für alle Netzwerkangehörigen) geknackt und statistisch ausgewertet.

(Hashing ist eine Methode zur Speicherung von Passwörtern. Dabei wird jedes Passwort durch eine eindeutige Zeichenkette, dem Hashwert, repräsentiert. Auch wenn Unbefugte diesen Wert erlangen, können sie das Passwort nicht reproduzieren.)

Durch Hash-Knacken können Sicherheitsprüfer schwache Passwörter – und dadurch Schwächen in der generellen Passwortwahl – identifizieren.

Eine Methode ist der sogenannte Brute-Force-Angriff, bei dem durch das einfache Ausprobieren verschiedener Eingaben versucht wird, den Hashwert zu reproduzieren. Umso einfacher ein Passwort gestaltet wurde, umso schneller lässt es sich knacken.

Statistische Analyse im Passwortaudit

Die statistische Auswertung enthüllt Muster und Trends in der Passwortwahl, die als Grundlage für verbesserte Passwortrichtlinien und Benutzerschulungen dienen können.

Dieser Prozess unterstützt das Unternehmen dabei, robustere Sicherheitsmaßnahmen einzuführen und die Integrität des Active Directory zu stärken.

Treecha | stock.adobe.com

WEBANWENDUNGS- UND SOFTWARECHECK

Die Sicherheitsprüfung einer Webanwendung ist darauf ausgerichtet, potenzielle Schwachstellen und Sicherheitslücken in einer Website und deren zugrunde liegenden Programmierung zu identifizieren.

Eine Kombination aus Penetrationstest und Secure Code Review gewährleistet eine umfassende Sicherheitsbewertung, die nicht nur externe Bedrohungen berücksichtigt, sondern auch interne Schwachstellen in der Anwendungslogik und im Code aufdeckt.

Sicherheitsprüfer nutzen dafür verschiedene Methoden, einschließlich automatisierter Scans und manueller Tests. Durch die Simulation von Angriffsszenarien – wie SQL-Injektionen oder Cross-Site Scripting (XSS) – wird getestet, ob ein Angreifer Zugang zu vertraulichen Daten oder Kontrollübernahmen erlangen kann.

Während der Penetrationstest darauf abzielt, Schwachstellen durch aktive Angriffe zu identifizieren, konzentriert sich ein Secure Code Review auf eine tiefgehende Analyse des Quellcodes. Durch diesen Prozess können potenzielle Sicherheitslücken, die in der Programmierung selbst begründet sind, aufgedeckt werden.

Dabei werden Designentscheidungen, Datenvalidierungsmethoden, Authentifizierungssysteme und weitere kritische Elemente geprüft. Hiermit wird sichergestellt, dass die Anwendung von Anfang an auf eine robuste und sichere Weise entwickelt wurde.

Ein abschließender Bericht enthält Empfehlungen zur Behebung der gefundenen Schwachstellen und zur Verbesserung der Gesamtsicherheit der Webanwendung.

Lücken im Code schließen.

ANGRIFFE VERHINDERN.

HAUPTEINFALLSTOR E-MAIL PHISHINGANGRIFFE

Mehr als 90 Prozent der Sicherheitsverletzungen in Unternehmen lassen sich auf Phishingangriffe zurückführen (Quelle: CSO Deutschland). Darunter versteht man den Diebstahl geistigen Eigentums oder persönlicher Daten durch fingierte E-Mails, Websites oder Direktnachrichten. Ziel ist es, Sie zu schädlichen Aktionen wie das Einloggen in einen gefälschten Webauftritt zu bewegen, um Ihre Zugangsdaten zu erhalten.

Ähnlich funktioniert (E-Mail-)Spoofing, wobei E-Mail-Adressen bekannter Personen nachgeahmt werden, um Mitarbeitende eines Unternehmens zu täuschen und sensible Daten oder finanzielle Mittel zu erschleichen. Auch Ransomware-Attacken, die Daten auf Ihrem Gerät sperren, um Lösegeld zu erhalten, sind weit verbreitet.

Wir bieten Trainings und Schulungen an, um Ihre Mitarbeitenden über diese Betrugsmaschen aufzuklären und über die richtigen Handlungsweisen bei erfolgreichen Täuschungen zu informieren.

Bewusstsein stärken.

BETRUGSVERSUCHE ERKENNEN.

PHISHINGSIMULATION

Um festzustellen, inwieweit Ihre Mitarbeitenden bereits für Phishing sensibilisiert sind, bieten wir Phishingsimulationen an.

Zur Auswahl stehen Ihnen drei Testpakete unterschiedlicher Laufzeiten. In drei bis viertägigen Phishingkampagnen testen wir die Reaktion Ihrer Mitarbeitenden auf fingierte E-Mails. Inhalte können aus vorbereiteten Vorlagen und jeweils unterschiedlichen Szenarien gewählt werden.

Sollten Mitarbeitende interagieren – indem Sie beispielsweise Links klicken oder Zugangsdaten eingeben – werden sie auf eine Warnseite weitergeleitet.

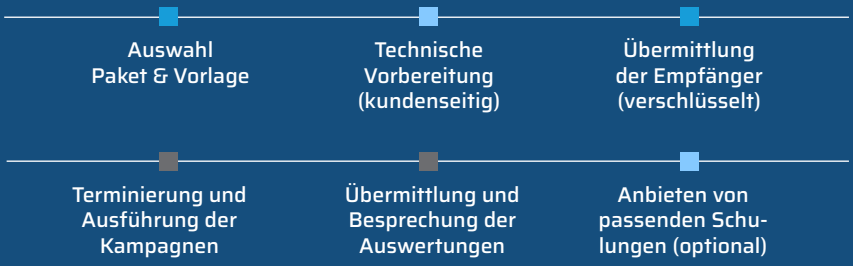
Auswertungen können wahlweise nach jeder Kampagne oder nach der Gesamtlaufzeit erfolgen. Betrachtet werden folgende Parameter:

- Öffnungsrate der E-Mails
- Anzahl der Linkklicks
- Eingabe von Zugangsdaten
- Aktivierung von Makros in zugesendeten Dokumenten
- Prozentuale Auswertung anhand aller Empfänger

PAKETE

Paket 1	*Paket 2*	*Paket 3*
4 Wochen	3 Monate	6 Monate
1 – 2 Kampagnen	4 – 6 Kampagnen	6 – 8 Kampagnen

ABLAUF



- Aktionen des Kunden
- Aktionen des Campus Vilshofen
- Gemeinsame Aktionen

SERVICES, FORSCHUNG UND INDIVIDUELLE BERATUNG

Sichern Sie Ihr Unternehmen.

Sie konnten nun einen kleinen Einblick in die Arbeit am Campus Vilshofen gewinnen. Die beschriebenen Services decken die am häufigsten geäußerten Sicherheitsbedenken ab – gerne beraten wir Sie individuell zu weiteren Themen und Leistungen.

Das Expert:innenteam hat sich auch im Bereich Forschung dem Thema Cybersicherheit verschrieben. Mit unseren weiteren Kernkompetenzen Künstliche Intelligenz und Angewandte Kryptographie betreiben wir Auftragsforschung für Unternehmen und führen Forschungsprojekte im Rahmen öffentlich geförderter Programme durch.

Sie möchten eine persönliche Beratung zu unseren Services oder sind an einer Forschungskooperation mit uns interessiert?

Kontaktieren Sie uns!

Mehr Informationen

putilov_denis | stock.adobe.com

Cybersicherheit – Beratung, Forschung, Services

Technische Hochschule Deggendorf

Campus Vilshofen
Aidenbacher Straße 32
94474 Vilshofen an der Donau
Deutschland

tcv-itsecurity@th-deg.de

www.th-deg.de/tc-vilshofen