

Cyberangriffe in der Wissenschaft – Digitalisierung als Gefahr und Chance

Thorsten Meyer, 26.01.2024

Bibs & Bits – Digitale Transformation in Bibliotheken



Cyberangriff auf Webseiten des Landes - russische Gruppe?

Stand: 05.04.2023 06:05 Uhr

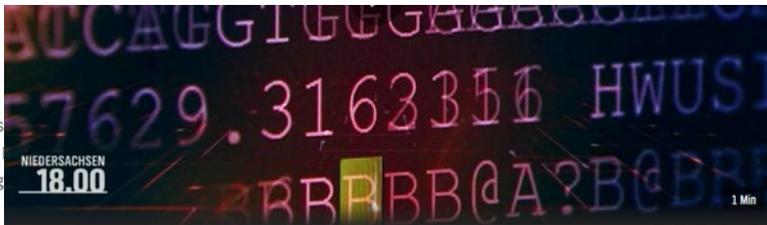
Nach dem Cyberangriff auf mehrere Internetseiten von Regierung und Behörden in Mecklenburg-Vorpommern ermittelt jetzt die Polizei. Betroffen waren mehrere Bundesländer, darunter auch Niedersachsen. Hinter den Angriffen steckt offenbar eine russische Gruppe.



Cyberangriff auf Webseiten des Landes - russische Gruppe?

Stand: 05.04.2023 06:05 Uhr

Nach dem Cyberangriff auf mehrere Internets
Mecklenburg-Vorpommern ermittelt jetzt die
darunter auch Niedersachsen. Hinter den Ang



Cyberangriff auf Polizei: Steckt pro-russische Gruppe dahinter?

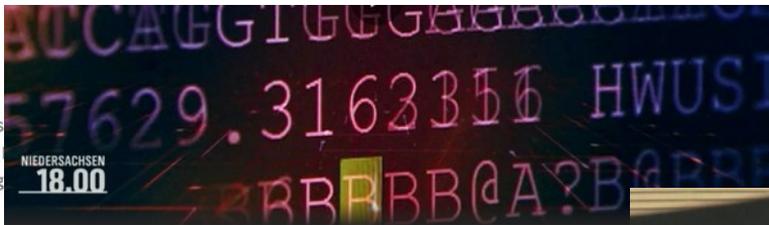
Stand: 05.04.2023 19:56 Uhr



Cyberangriff auf Webseiten des Landes - russische Gruppe?

Stand: 05.04.2023 06:05 Uhr

Nach dem Cyberangriff auf mehrere Internets... Mecklenburg-Vorpommern ermittelt jetzt die... darunter auch Niedersachsen. Hinter den Ang...



Cyberangriff auf Polizei: Steckt pro-russische Gruppe dahinter?

Stand: 05.04.2023 19:56 Uhr



Cyberangriffe in SH: Ermittler suchen die "Haarspitze"

Stand: 26.04.2023 17:00 Uhr

Cyberangriffe aufs Landesportal, das Leibniz-Informationzentrum Wirtschaft und auf Werften - alles in Schleswig-Holstein passiert, alles in den vergangenen Wochen. Die Suche nach den Hintermännern gestaltet sich mühsam.

ANGRIFF AUF DIE IT-INFRASTRUKTUR

ANGRIFF IT-INFRA



Uni Duisburg-Essen: Hacker drohen mit Veröffentlichung von Daten

Stand: 29.11.2022, 17:54 Uhr

Nach dem Hackerangriff auf die Uni Duisburg-Essen liegt die IT-Infrastruktur weiter fast vollständig brach. Die Erpresser drohen damit, sensible Daten im Darknet zu veröffentlichen.

ANGRIFF IT-INFRA



Uni Duisburg-Essen: Hacker- chung von Daten

Stand: 29.11.2022, 17:54 Uhr

Nach dem Hackerangriff auf die Uni Duis-
burg weiter fast vollständig brach. Die Erpress-
Darknet zu veröffentlichen.

Cyberangriff auf das DIPF: Aktueller Stand



@pixelio

25.07.2023

Nach dem Cyberangriff auf das DIPF sind inzwischen viele, jedoch nicht alle Dienste
wiederhergestellt worden. Die Kolleg*innen arbeiten weiterhin am Wiederaufbau

ANGRIFF IT-INFRA



Uni Duisburg-Essen: Hacker- chung von Daten

Stand: 29.11.2022, 17:54 Uhr

Nach dem Hackerangriff auf die Uni Duis-
burg weiter fast vollständig brach. Die Erpress-
er Darknet zu veröffentlichen.

Cyberangriff auf das DIPF: Aktueller Stand



25.07.2023

Nach dem Cyberangriff auf das DIPF s-
ystem wiederhergestellt worden. Die Kolleg*
innen

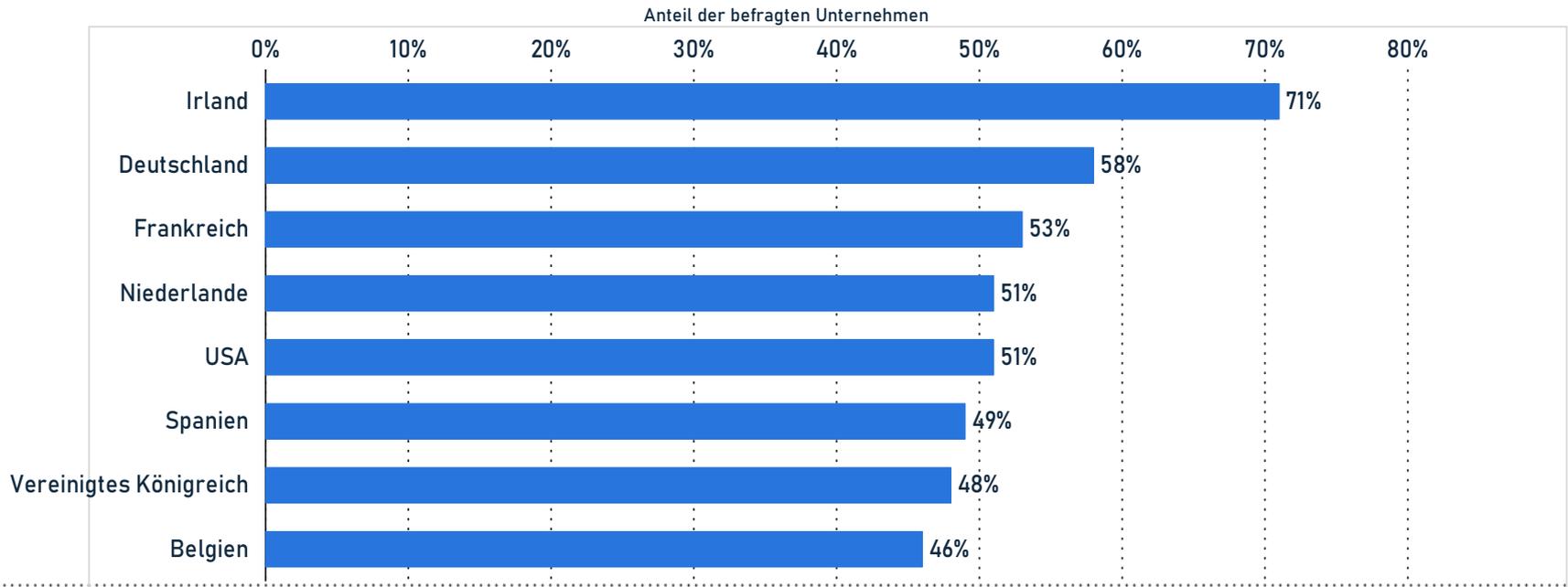
HZB blogcampus

CYBERANGRIFF AUF DAS HELMHOLTZ-ZENTRUM BERLIN

By: Silvia Zerbe | On: 16. Juni 2023 | In: Internationales, Mitarbeiter



Anteil der Unternehmen, die in den letzten 12 Monaten eine Cyber-Attacke erlebt haben, in ausgewählten Ländern im Jahr 2023





223 Milliarden Euro Schaden durch Cyberangriffe

Die deutsche Wirtschaft ist aktuell mehr denn je von Cyberangriffen betroffen. Insgesamt 223 Milliarden Euro beträgt der wirtschaftliche Schaden, welcher im vorangegangenen Jahr durch Cyberattacken in Deutschland verursacht wurde. Dies geht aus einer Studie des Digitalverbands Bitkom hervor, für die mehr als 1000 Unternehmen aus unterschiedlichen Branchen befragt wurden.

Welche häufigen Arten von Cyberangriffen gibt es?

Phishing

Distributed Denial of Service

Ransomware

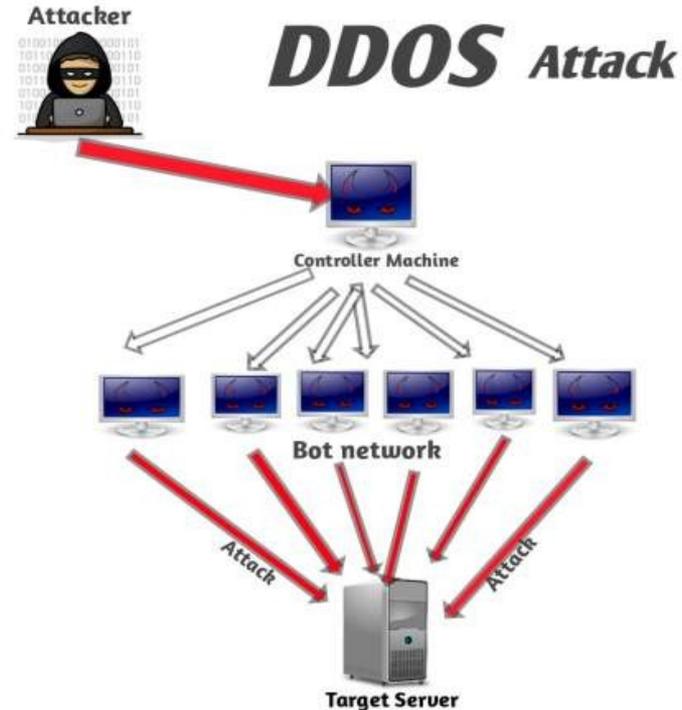


Welche häufigen Arten von Cyberangriffen gibt es?

Phishing

Distributed Denial of Service

Ransomware



Welche häufigen Arten von Cyberangriffen gibt es?

Phishing

Distributed Denial of Service

Ransomware



Cyberangriff auf die ZBW: Was ist passiert?

Gruppe Royal

~01.04.2023

Eindringen in IT-
Infrastruktur

Nacht 04-05.04.2023

Angriff auf IT der ZBW

Erstmaßnahmen der ZBW:

- geordnetes Abschalten aller Microsoft- und Linuxsysteme
 - Abschaltung der Internetzugänge
 - Einbeziehung des LKA Schleswig-Holstein, Erstattung Strafanzeige
 - Meldung beim Unabhängigen Landeszentrum für Datenschutz
 - Information an das Bundesamt für Sicherheit in der Informationstechnik (BSI)
 - Notfallkommunikation mit Beschäftigten
 - Incident-Response-Service für Forensik beauftragt
-

Lösegeldforderung

Hello!

If you are reading this, it means that your system were hit by Royal ransomware.
Please contact us via :
<http://royal2>

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 and even your employees will be able to see your internal documentation: personal data, HR reviews, internal lawsuits and com

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 covering you from reputational, legal, financial, regulatory, and insurance risks, but will also provide you with a security To put it simply, your files will be decrypted, your data restored and 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!

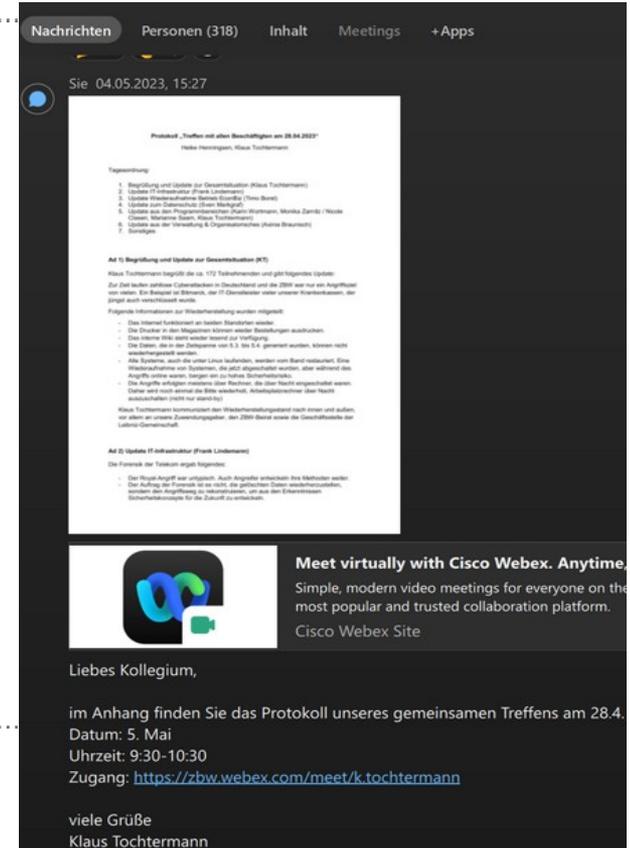
Wie erreiche ich 300 Beschäftigte ?

Chat für alle Beschäftigte

ZBW-Notfallseite auf der Homepage

Jeden Freitag virtuelle Informations-
veranstaltung für alle Beschäftigte

Kontinuierlicher Dialog mit Personalrat
und Datenschutzbeauftragtem



Was ist von einem Cyberangriff betroffen?

Verschlüsselung von Infrastruktur, die auf Microsoft-Produkten basiert:

- E-Mail-Server
- interne Laufwerke mit Arbeitsdokumenten
- Festplatte zur Datensicherung, Bänder der Tape-Library
- Active Directory (Liste Nutzerzugänge)
- Interne Infrastrukturkomponenten (VPN, Back-up, Softwaremanagement etc.)

Linux-Systeme waren nicht betroffen.

Services für Nutzer:innen – ZBW blieb handlungsfähig

The screenshot shows the ZBW website homepage with the following content:

- Navigation:** Impressum | Kontakt | Karriere | FAQ | Leichte Sprache | Barrierefreiheit | English
- Search:** Webseitensuche
- Header:** ZBW Leibniz-Informationszentrum Wirtschaft Leibniz Information Centre for Economics
- Main Text:** Leibniz-Informationszentrum Wirtschaft Ihr Partner für Forschung und Studium
- Left Sidebar:** RECHERCHIEREN, PUBLIZIEREN, SERVICE, FORSCHUNG, OPEN SCIENCE, FORSCHUNGSDATEN, WISSENSCHAFTSPOLITIK, WISSENSTRANSFER, ÜBER DIE ZBW
- RECHERCHIEREN:** ZBW IST OFFLINE
Die ZBW ist einem Cyberangriff zum Opfer gefallen. Zahlreiche Services inklusive unserer bekannten E-Mail-Adressen sind derzeit nicht erreichbar. Davon nicht betroffen sind unsere extern gehosteten Dienste, wie z.B. Wirtschaftsdienst, Intereconomics, STW.
Sie erreichen uns aktuell unter folgender E-Mail: zbw@zbw-workspace.eu
- RECHERCHIEREN:** Wirtschaftsliteratur weltweit suchen im Fachportal EconBiz:
[In EconBiz suchen] [suchen]
➤ Online anmelden & ZBW-Nutzer:in werden
➤ ZBW-Konto einsehen
- ZBW AKTUELL:**
 - NDR-Bericht zum Cyber-Angriff auf die ZBW
Lesetipp: 21.04.2023 | Aktuell
 - Partnerschaftlicher Umgang mit Forschungsdaten
Schleswig-holsteinische Hochschulen und Forschungseinrichtungen stellen gemeinsames Konzept vor
20.04.2023 | Pressemitteilung
 - ChatGPT & Co.: Wenn der Suchschlitz zur KI-Chatbox wird
Neues aus dem ZBW Media Talk.
16.03.2023 | ZBW Media Talk
 - 5. Workshop Retrodigitalisierung: Umgang mit Materialien aus schwierigen Zusammenhängen - Ethische, rechtliche Aspekte und daraus folgende technische Aspekte der Digitalisierung
11.-12. Mai 2023, ZBW Kiel.
16.03.2023 | Workshops
- Footer:** PUBLIZIEREN

- Homepage, Wirtschaftsdienst, Intereconomics nicht beeinträchtigt
- Bibliotheksbetrieb vor Ort seit 12. April 2023
- EconBiz, Econstor seit 8. Mai wieder online (70%-80% des Nutzungsniveaus)
- Alle online-Angebote seit 16.5. wieder in Betrieb

Was macht die ZBW schnell wieder handlungsfähig? (1/2)

- Verteilte IT-Infrastruktur, Betrieb in-house, Hosting, Cloud
 - Homepage zbw.eu, Webex, Diamant R4, SD Worx
 - externer Betrieb der Bibliothekssysteme
- Dezentrale Speicherung von Administratoren-Zugängen
- Datensicherungsstrategie (für Daten & Systeme)
- Verteilt abgelegtes IT-Notfallhandbuch

Was macht die ZBW schnell wieder handlungsfähig? (2/2)

- Internetzugang war durchgängig vorhanden (externer Anbieter)
- vorhandene Kommunikationsinfrastruktur für Notfälle
- schnelle Schaffung provisorischer Arbeitsumgebungen durch Nutzung bereits vorhandener alternativer Infrastruktur
- laufende Investition in IT-Infrastruktur und IT-Sicherheit

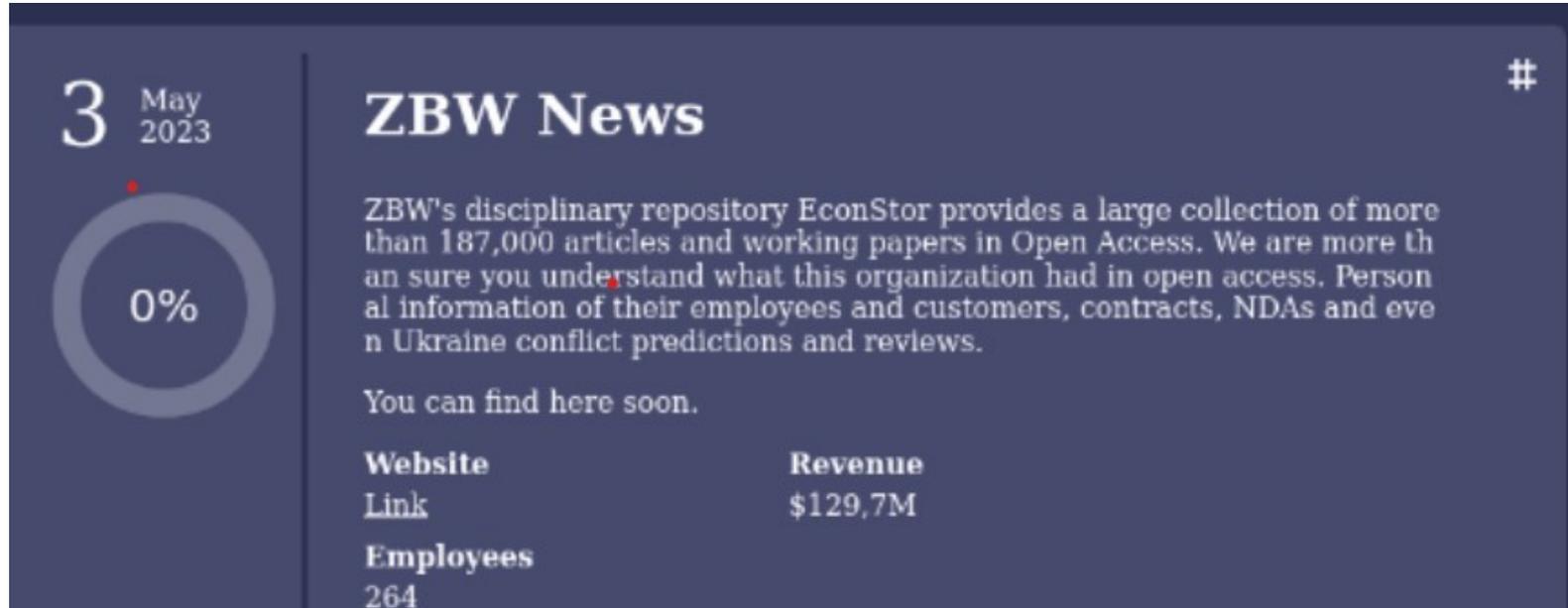
Sehr große Flexibilität und Ideenreichtum des Kollegiums

Datenverlust

- Arbeitsdokumente aus dem Zeitraum 5. März bis 5. April
- Verwaltungsdokumente (z.B. Informationen über Beschäftigte)
- Keine personenbezogenen von Nutzenden (gehostet in Göttingen bei der VZG)
- Hohe Wahrscheinlichkeit, dass Daten auch abgeflossen sind

Datenveröffentlichung im Darknet?

Voraussichtlich auf Leakseite von Royal



Datenveröffentlichung im Darknet?

Voraussichtlich auf Leakseite von Royal

**Sehr wahrscheinlich nicht mehr aktuell,
Leakseite verschwunden**

Erhöhung des Sicherheitsniveaus

- Gut geschulte, sensibilisierte Beschäftigte
- Starke Passwörter
- Modernste Scansoftware zum Erkennen schadhafter Software

2.1 Allgemeine Passwort Anforderungen

- Das Passwort muss mindestens 12 Zeichen lang sein (maximal 30 Zeichen).
- Erlaubte Zeichensätze:
 - Großbuchstaben: A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z
 - Kleinbuchstaben: a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z
 - Ziffern: 0,1,2,3,4,5,6,7,8,9
 - Sonderzeichen: ! " \$ % & ' () * + , - . / ; < = > ? { | } ~] @
- Es dürfen keine persönlichen Daten, Namen oder die Kennung von Nutzenden enthalten sein.

Erhöhung des Sicherheitsniveaus

- Multifaktor-Authentifizierung
- keine zu starke Zentralisierung der IT-Infrastruktur
- Penetrationstests
- Netzwerk mit mehreren Netzwerksegmenten
- Vorhalten einer Datensicherungsstrategie

Vielen Dank für Ihre Aufmerksamkeit!

Thorsten Meyer

t.meyer@zbw-online.eu

Cyberkriminalität kann alle Einrichtungen treffen. Es ist längst keine Frage mehr des „ob“, sondern des „wann“.