

bayern  innovativ

ZD.B ZENTRUM
DIGITALISIERUNG.
BAYERN



Datenschutz und IT-Sicherheit im Homeoffice

Bianca Sum & Dominik Golle

Verhaltens- und Complianceregeln

- Ein Aufzeichnen (und die Wiedergabe) des Webinars ist nicht gestattet.
- Verbreiten und kommunizieren Sie keine vertraulichen oder kartellrechtlich relevanten Informationen (z.B. Preisinformationen) über den Chat. Der Chatverlauf wird protokolliert.
- Stellen Sie Ihre Fragen bitte über die Chatfunktion.
- **Dieses Webinar ist ein unverbindliches Informationsangebot und stellt keine Rechtsberatung dar. Alle hier dargestellten Informationen sind ohne Gewähr auf Richtigkeit und Vollständigkeit.**

Referent*innen



Bianca Sum
Leitung Themenplattform
Cybersecurity

bianca.sum@zd-b.de
089-2488071-23



Dominik Golle
Leitung Themenplattform
Verbraucherbelange

dominik.golle@zd-b.de
089-2488071-15



Eine Initiative von
Bayerisches Staatsministerium für
Umwelt und Verbraucherschutz



Themenplattform Verbraucherbelange in der Digitalisierung



Image via www.vpnrus.com



Wie gut ist Ihr Unternehmen auf Remote Work eingestellt?

- Nutzen Sie einen dienstlichen Laptop oder private Geräte?
- Gibt es eine zuständige Person für IT-Sicherheit?
- Gibt es eine zuständige Person für Datenschutz?
- Gibt es eine Richtlinie Datenschutz und IT-Sicherheit im Homeoffice?

Cybercrime nimmt zu während der Corona-Pandemie

Täglich 2600 Fälle: Cyber-Attacken mit Coronavirus-Bezug boomen

Das [Coronavirus](#) bestimmt dieser Tage unser Leben, Arbeit und Freizeit spielen sich zu einem großen Teil im Internet ab. Das wissen auch Online-Betrüger und versuchen, das auszunutzen. Denn täglich werden mehr als 2600 Attacken registriert, die Bezug zu Covid-19 herstellen.

IT-SICHERHEIT

Der perfekte Köder: Cyberkriminelle nutzen die Corona-Panik

Die Coronavirus-Krise ist für die Angreifer besonders geeignet. Experten rechnen mit einem starken Anstieg der kriminellen Aktivitäten.

Cybersicherheit: 85 Prozent Plus bei Corona-Domains in letzter Woche – 16.000 seit Januar

30. März 2020, Autor: [Michael Kroker](#)

In den vergangenen drei Wochen wurden zehnmals mehr Internet-Domains mit Bezug zum Coronavirus registriert als in Januar und Februar zusammen – die Mehrzahl davon mit betrügerischer Absicht.

Nach Cyberangriff auf tschechisches Spital warnt auch der Bund vor Attacken

Kriminelle nutzen die Corona-Pandemie für Betrügereien und Cyberangriffe aus. Direkte Attacken auf Spitäler sind dabei nur eine von vielen Gefahren. Der Bund hat sein Monitoring verstärkt.

Quellen:

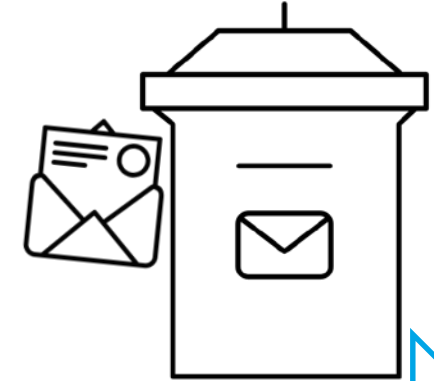
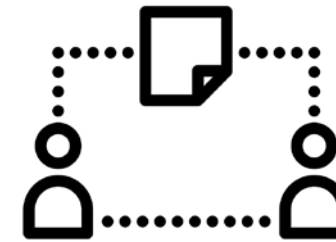
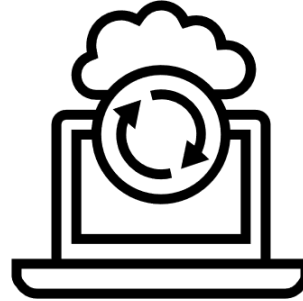
<https://winfuture.de/news,115135.html>

<https://www.nzz.ch/schweiz/nach-cyberangriff-auf-tschechisches-spital-warnt-auch-der-bund-vor-attacken-ld.1546736>

<https://blog.wiwo.de/look-at-it/2020/03/30/cybersicherheit-85-prozent-plus-bei-corona-domains-in-letzter-woche-16-000-seit-januar/>

<https://www.handelsblatt.com/technik/it-internet/it-sicherheit-der-perfekte-koeder-cyberkriminelle-nutzen-die-corona-panik/25641346.html>

Der ideale Homeoffice-Tag aus IT-Sicherheits- und Datenschutzperspektive



Tipps für mehr Datenschutz und IT-Sicherheit im Home Office

Wichtig: Sensibilisieren Sie alle Mitarbeiter*innen für das Thema Datenschutz und IT-Sicherheit!

Datenschutz

- Eigenes Arbeitszimmer bzw. Arbeitsbereich, Sichtschutzfolie, Unterlagen einschließen
- Bei Nutzung privater Geräte:
 - Mitarbeiter*innen zu regelmäßigen Updates und datenschutzfreundlichen Systemeinstellungen (insb. Windows & Office 365) verpflichten
 - Ausschließlich Web Client für Emails erlauben
- Bei allen Tools zur Kollaboration und Kommunikation auf Datenschutz achten – oft gibt es zu den Diensten datenschutzrechtliche Einschätzungen im Internet. Open Source Lösungen: Jitsi, Mattermost, Signal, Cryptpad
- Zuständigkeit für Datenschutz im Unternehmen benennen und kommunizieren
- Verbindliche und sanktionsbewehrte Richtlinie zu Datenschutz und IT-Sicherheit im Home Office erlassen

IT-Sicherheit

- Sichere Passwörter verwenden (auch fürs WLAN zu Hause!): Erklärvideo Passwortsicherheit <https://youtu.be/xnNgd3AvnqU>
- Passwortmanager verwenden, z.B. KeePass, 1Password, Keeper Security etc.
- Wenn möglich VPN Client nutzen
- Programme aktuell halten, Updates durchführen, Virenschutz (automatisch) aktualisieren
- Vorsicht beim Öffnen und Bearbeiten von E-Mails (z.B. auch mit Corona-Bezug): Erklärvideo Phishing <https://youtu.be/IR0UM33botU>
- Backups regelmäßig erstellen: Erklärvideo Datensicherung <https://youtu.be/zXyAOu6AQYk>
- Vorbereitung für den Notfall: Erklärvideo IT-Notfallplan <https://youtu.be/xInmVijCYwA>
- Zuständigkeit für IT-Sicherheit im Unternehmen benennen und kommunizieren

- ZD.B-Erklärvideo Passwortsicherheit: <https://youtu.be/xnNgd3AvnqU>
- ZD.B-Erklärvideo Phishing: <https://youtu.be/IR0UM33botU>
- ZD.B-Erklärvideo Datensicherung: <https://youtu.be/zXyAOu6AQYk>
- ZD.B-Erklärvideo IT-Notfallplan: <https://youtu.be/xInmViiCYwA>
- Plötzlich Homeoffice, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD): <https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf>
- Home-Office? - Aber sicher!, Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.html
- Top Tips for Cybersecurity when Working Remotely, European Union Agency for Cybersecurity (ENISA): <https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely>
- Telearbeit und Mobiles Arbeiten, Information des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI): <https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html>
- Microsoft Security & Compliance Portal: <https://protection.office.com/homepage>
- Microsoft Service Trust Portal: <https://servicetrust.microsoft.com>
- Anleitung für datenschutzfreundliche Einstellungen bei Office 365: z.B. <https://www.buero-kaizen.de/datenschutz-und-dsgvo-bei-microsoft-office-365/>
- Rechtliche Grundlagen: Datenschutz und IT-Sicherheit Im Homeoffice, Heise online: <https://www.heise.de/newsticker/meldung/Datenschutz-und-Datensicherheit-im-Homeoffice-4698301.html>

Fragen und Antworten

Weitere Termine der Webinarreihe „Arbeitswelt 4.0“

Dienstag 21. April, 10:00 Uhr, **Zeit- und Selbstmanagement im Homeoffice**

Donnerstag 23. April, 10:00 Uhr, **Mentale Gesundheit im Homeoffice**

Dienstag 28. April, 10:00 Uhr, **Digitalisierung von Geschäftsmodellen**

Donnerstag 30. April, 10:00 Uhr, **Digitales Lernen in die Organisation bringen – Einstieg**

Dienstag 5. Mai, 10:00 Uhr, **Führen und Zusammenarbeit in virtuellen Teams**

Donnerstag 7. Mai, 10:00 Uhr, **Wissensmanagement in virtuellen Teams**

Dienstag 12. Mai, 10:00 Uhr, **Resilienz in Krisenzeiten**

Anmeldung bitte per E-Mail an arbeitswelt4.0@zd-b.de oder an michael.schalk@vdma.org

Vielen Dank für Ihre Aufmerksamkeit!



Dr. Imme Witzel

Projektmanagerin Technologie
Leiterin ZD.B-Themenplattform
Arbeitswelt 4.0
T +49 89 248807 162
arbeitswelt4.0@zd-b.de



Michael Schalk

Projektmanager Industrie 4.0
VDMA Landesverband Bayern
T +49 89 27828761
michael.schalk@vdma.org

Gefördert durch



Bayerisches Staatsministerium für
Familie, Arbeit und Soziales

Gefördert durch



Bayerisches Staatsministerium für
Wirtschaft, Landesentwicklung und Energie