Cyber-Sicher durch die Krise

Krisenzeiten sind Zeiten der Veränderung – und damit auch für die IT-Sicherheit kritisch. Wie Sie cyber-sicher durch die Krise kommen und was in Ihrem Unternehmen aktuell noch beachtet werden sollte, zeigt Ihnen das **Cyber Security Cluster Bonn** in den folgenden Kapiteln.

CYBER SECURITY CLUSTER BONN

@CSCBonn

https://cyber-security-cluster.eu

Zur aktuellen Situation

Das Coronavirus hält die Welt in Atem und es ist nicht überraschend, dass auch Betrüger versuchen, die aktuelle Situation für ihre Zwecke auszunutzen. Im Rahmen der zu bewältigenden Herausforderungen gilt es für viele Unternehmen, ihre Mitarbeiter schnellstmöglich in die Lage zu versetzen, aus dem Home-Office heraus zu arbeiten, um Ansteckungsgefahren zu minimieren. Hier ergeben sich neben administrativen Themen auch Herausforderungen im Bereich der Cyber-Sicherheit.

Durch die aktuelle Situation kommt es zu einer verstärkten Nutzung des Internets – ob beruflich oder privat. Gerade neue und für Nutzer noch wenig vertraute Aktivitäten werden von Cyber-Kriminellen gern ausgenutzt, indem sie z.B. auf die Situation adaptierte Phishing- und andere Angriffe auf Unternehmensnetzwerke initiieren oder Fake-Shops – etwa mit Angeboten medizinischer Produkte – eröffnen.

Ein kritisches Auge und regelmäßige Informationen zu neueren Entwicklungen helfen gerade in hektischen Zeiten. Das Coronavirus mag offline wüten, macht aber auch vor der digitalen Welt nicht Halt. Bleiben Sie wachsam und informieren Sie bei verdächtigen Aktivitäten unmittelbar die zuständigen Ansprechpartner in Ihrem Unternehmen.

Themen-Überblick

Für alle Mitarbeiter

1. Allgemeine Grundlagen – Was Sie sofort umsetzen können
2. Phishing / Spam-Mails / CEO-Fraud – Auch Kriminelle verstehen die Krise als Chance
3. Gesund im Home-Office – Selbstorganisation am Heimarbeitsplatz
4. Sicher Lernen mit digitalen Medien – Wie der Einsatz zu Hause gelingt

Für IT-Verantwortliche

5. Klare Kommunikationswege – Konkrete Ansprechpartner für Mitarbeiter
6. Videokonferenz Systeme – Vergleich häufig genutzter Tools
7. Sonstiges – Weitere Empfehlungen

Cyber-Sicher durch die Krise – Kapitel 1

Allgemeine Grundlagen

Vor Allem durch die schnelle Umstellung auf Home-Office Arbeitsplätze ergeben sich für viele Unternehmen und Mitarbeiter momentan neue Herausforderungen. Was Sie an Ihrem Arbeitsplatz sofort umsetzen können und sollten, zeigen wir Ihnen hier.

CYBER SECURITY CLUSTER BONN

Was Sie sofort umsetzen können

Aktivieren Sie den Passwortschutz Ihres PCs oder Laptops.

Sperren Sie bei Abwesenheit **den Bildschirm**.

Schalten Sie **sprachgesteuerte Geräte** (z.B. Alexa oder Siri) während der Arbeit aus.

Was Sie sofort umsetzen können

Verwenden Sie eine **Webcam-Abdeckung**, wenn die Webcam nicht in Nutzung ist. **Richten** Sie Ihren **Bildschirm** idealerweise **nicht Richtung Fenster aus**, gerade wenn Sie im EG wohnen. In jedem Fall beugt eine rechtwinklige Ausrichtung des Monitors zum Fenster Reflexionen vor, die für die Augen anstrengend sind.

Halten Sie Ihre **Software auf dem neuesten Stand**. Aktualisieren Sie ggf. Ihr **Betriebssystem,** die von Ihnen genutzten **Programme** und prüfen Sie beispielsweise auch, ob für Ihren **Router** ein **Update** vorliegt.

Aktivieren Sie den **Virenscanner** (z.B. der in Windows integrierte Defender) und halten Sie **Antivirus-Signaturen** auf dem neusten Stand.

Was Sie sofort umsetzen können

Prüfen Sie, ob die in Ihrem Betriebssystem integrierte **Firewall aktiviert** ist.

- Windows: Systemsteuerung → System → Sicherheit → Windows Defender Firewall
- Mac: Systemeinstellungen → Sicherheit → Klick auf den Reiter (oben) „Firewall“ → ggf. Firewall aktivieren

Verschlüsseln Sie Tragbare IT-Systeme und **Datenträger** (z.B. mit VeraCrypt, DiskCryptor oder FileVault). Besprechen Sie die Möglichkeiten mit dem IT-Ansprechpartner Ihres Unternehmens.

Nutzen Sie **für jeden Account ein anderes, sicheres, Passwort**. Bei Bedarf verwenden Sie einen **Passwortmanager** (z.B. Schlüsselbund (Mac), KeePass, Buttercup).

Schützen Sie Ihren **Router** sowie Ihr **WLAN gegen unbefugten Zugriff**. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet entsprechende Anleitungen.

Was Sie sofort umsetzen können

Aktivieren Sie wo immer möglich die **2 Faktoren-Authentisierung** (2FA): Bei der 2FA weisen Sie als Nutzer ihre Identität mittels der Kombination von zwei unabhängigen Komponenten (Faktoren) nach. Ein bekanntes Beispiele der 2FA ist die Nutzung von Login-Daten + Transaktionsnummer (TAN) beim Online-Banking.

Bei Ihrem **Microsoft-Konto aktivieren** Sie die **2FA** beispielsweise wie folgt:

- Loggen Sie sich in Ihr Microsoft-Konto ein unter https://office.com, klicken Sie rechts oben auf Ihre Initialen und wählen Sie „Mein Konto“
- Klicken Sie links auf „Sicherheit und Datenschutz“ und wählen Sie „Weitere Sicherheitsoptionen“
- Wählen Sie unter „Prüfung in zwei Schritten“ die Option „Prüfung in zwei Schritten einrichten“ und folgen Sie den Anweisungen

Nutzen Sie eine VPN Software, um sich **sicher mit Ihrem Unternehmensnetzwerk zu verbinden.** Wenden Sie sich für die Einrichtung an Ihren IT-Verantwortlichen.
Sie können sich eine **VPN** Verbindung wie einen **sicheren Tunnel zwischen Ihrem Rechner und Ihrem Unternehmensnetzwerk** vorstellen.
Auch das BSI gibt eine Anleitung zur Einrichtung.

Was Sie sofort umsetzen können

Nutzen Sie **unverschlüsselte, öffentliche WLAN Verbindungen** (z.B. im Park oder Zug) für dienstliche Zwecke nur **in Kombination mit aktiviertem VPN**. Im Zweifel verbinden Sie sich über das **mobile Netz** bzw. über Ihr **Smartphone als Hotspot** (LTE).

Speichern Sie Daten idealerweise stets auf den **zentralen Systemen Ihrer Institution** und nicht lokal. Falls Sie Daten dennoch lokal speichern wollen oder müssen, erstellen Sie regelmäßig **BackUps** (Sicherungskopien) von diesen.

Verstauen Sie nicht genutzte **Geräte sicher und schützen sie diese** vor fremden Zugriffen.

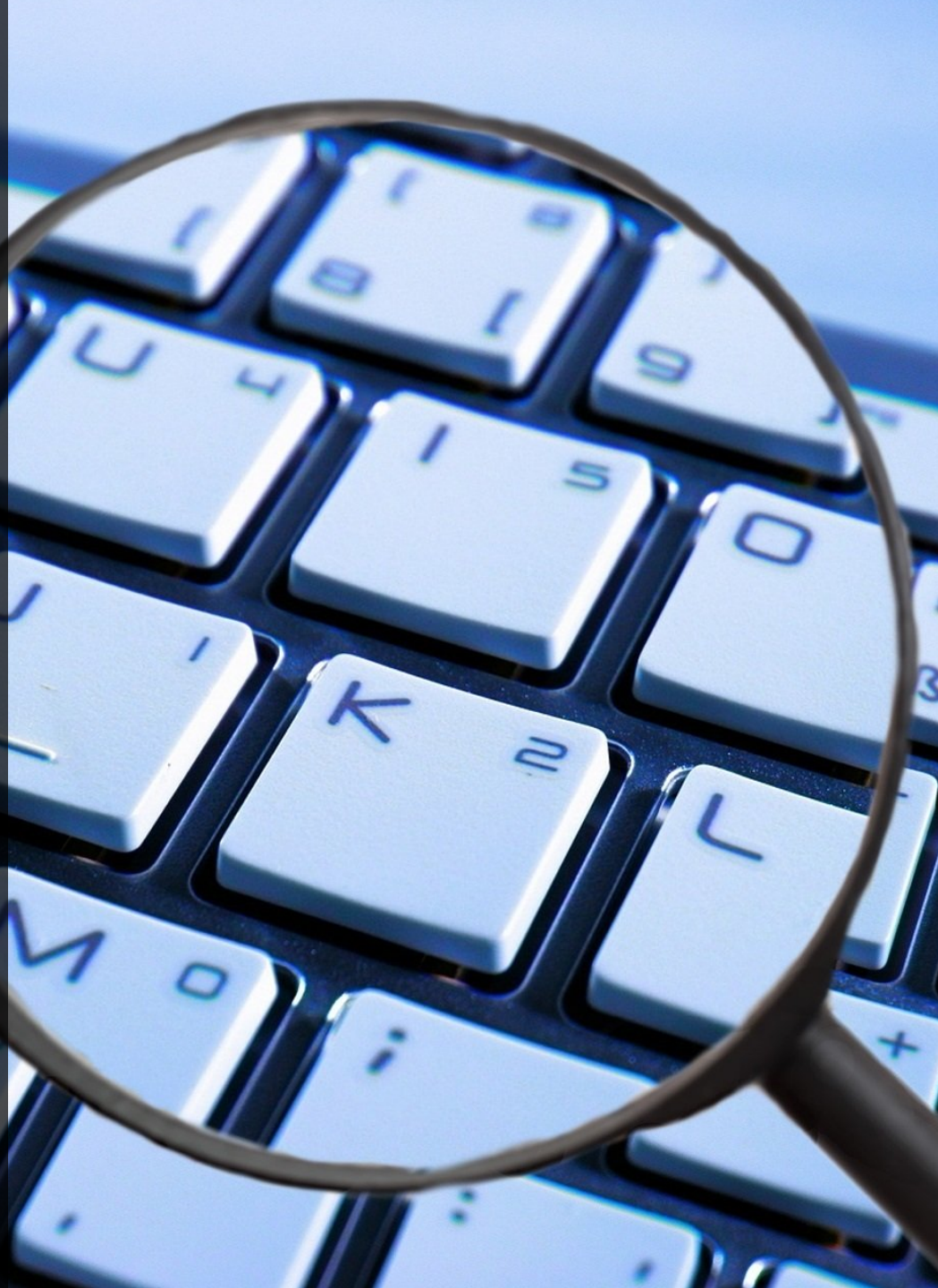
Halten Sie sich an die **Sicherheitsrichtlinien** Ihrer Institution. Fragen Sie im Zweifel die IT-Verantwortlichen und prüfen Sie Ihre Einstellungen beispielsweise anhand der Checkliste der Allianz für Cybersicherheit.

Cyber-Sicher durch die Krise – Kapitel 2

Phishing / Spam-Mails / CEO-Fraud

Auch Kriminelle verstehen die Krise als Chance und suchen neue Wege, um an sensible Daten zu gelangen. Wir erklären, was Sie tun können, um sich und Ihre Daten zu schützen.

CYBER SECURITY CLUSTER BONN



Auch Kriminelle verstehen die Krise als Chance

Durch die räumliche Trennung von Teams und Kollegen steigt die Erfolgswahrscheinlichkeit von **(Spear) Phishing**.

Daher gilt jetzt ganz besonders:

- Öffnen Sie **keine Anhänge** und **Links in E-Mails** von **unbekannten Absendern**
- Achten Sie auch bei E-Mails von **vermeintlich vertrauenswürdigen Absendern** auf **Unstimmigkeiten**
- Halten Sie **bei Unsicherheiten Rücksprache mit Ihrem Ansprechpartner**
- Seien Sie **besonders aufmerksam** auf **Websites mit Corona-Inhalt.** Derzeit gibt es etliche Corona-Fake-Websites, deren Zweck es ist, Daten abzugreifen oder Ihr System zu infizieren

Auch andere **Social Engineering Angriffe** wie der Versuch des „**CEO-Frauds“** – der **Betrüger gibt sich als Ihr Vorgesetzter aus** und fordert Sie zur Preisgabe sensibler Informationen auf – treten derzeit verstärkt auf. Geben Sie daher sensible Daten nie ohne Weiteres preis. **Verifizieren Sie potentiell kritische Aufforderungen** z.B. durch einen Rückruf.

Cyber-Sicher durch die Krise – Kapitel 3

Gesund im Home-Office

Die Arbeit im Home-Office sollte nicht zu Bewegungsmangel und dem Fehlen sozialer Kontakte führen. Wie Sie dem vorbeugen und wie Selbstorganisation am Heimarbeitsplatz gelingt, lesen Sie hier.

CYBER SECURITY CLUSTER BONN

Selbstorganisation am Heimarbeitsplatz

Richten Sie sich einen Arbeitsplatz ein und halten Sie diesen möglichst ordentlich. Falls möglich, nutzen Sie auch zu Hause ein **separates Arbeitszimmer** um Arbeit und Privates zu trennen.

Strukturieren Sie Ihren Home-Office-Tag und finden Sie Ihren **persönlichen Arbeits-Rhythmus**. Sofern möglich, passen Sie Ihre Arbeitszeiten an den Rhythmus an, in dem Sie am produktivsten arbeiten können.

Führen Sie Ihre Morgenroutine durch: Geben Sie Ihrem Kopf die Möglichkeit, in den Arbeitsmodus zu schalten, indem Sie sich wie gewohnt für die Arbeit fertig machen.

Auch im Büro arbeiten Sie keine acht Stunden am Stück. Tauschen Sie sich auch im Home-Office mit Kollegen aus, legen Sie **„gemeinsam“ Kaffeepausen** ein, **lüften Sie** regelmäßig und machen Sie Ihre **Mittagspause nicht am Arbeitsplatz**.

Selbstorganisation am Heimarbeitsplatz

Minimieren Sie Ablenkungen im Haushalt. Ihr privates Smartphone schalten Sie am besten stumm. Vielleicht erlaubt es Ihnen der Heim-Arbeitsplatz ja sogar, besonders fokussiert bei der Arbeit zu sein.

Trennen Sie Arbeitszeit und private Zeit: Setzen Sie sich selbst Grenzen und beenden Sie zu gegebener Zeit bewusst Ihren Arbeitstag.

Ernähren Sie sich gesund und **bringen Sie Bewegung in Ihren Home-Office-Tag.** Nutzen Sie beispielsweise die Zeit, die Sie sonst mit der Fahrt zur Arbeit verbringen.

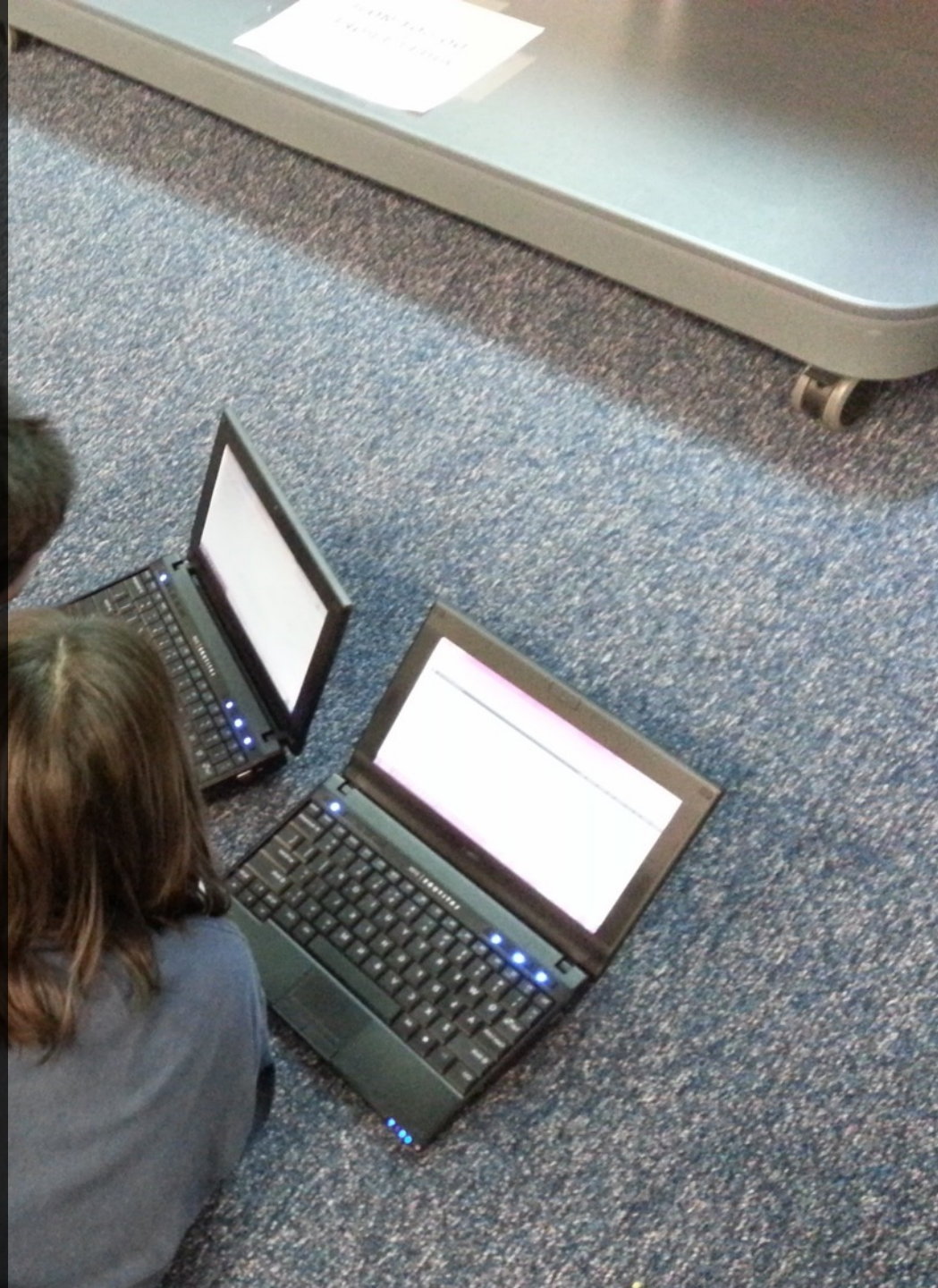
Tauschen Sie sich mit Kollegen und Vorgesetzten aus und scheuen Sie sich nicht, auch über persönliche Herausforderungen mit der Arbeit im Home-Office zu sprechen. Verwenden Sie zur Kommunikation nur Dienste, die Ihr Unternehmen autorisiert hat.

Cyber-Sicher durch die Krise – Kapitel 4

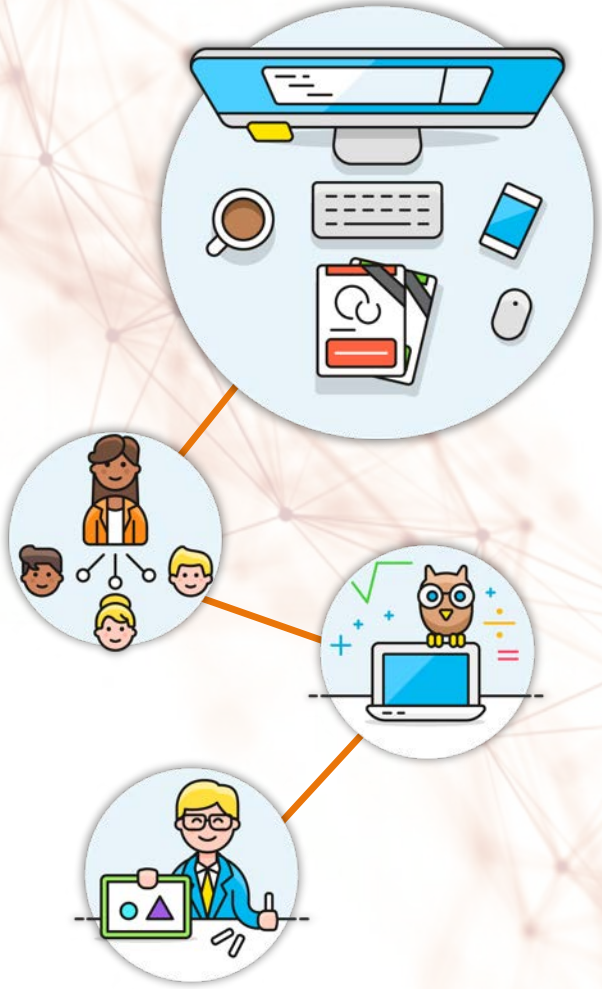
Sicher Lernen mit digitalen Medien

Aufgrund der aktuellen Schulschließungen müssen sich Kinder zu Hause mit den Inhalten des Unterrichts beschäftigen. Flankierend werden zusätzlich auch vermehrt digitale Dienste wie Wissens-Apps, Lernvideos und Online-Spiele genutzt. Wir geben Ihnen Tipps, wie sich das digitale Lernen zu Hause sicher umsetzen lässt.

CYBER SECURITY CLUSTER BONN



Wie der Einsatz zu Hause gelingt



Die **Aufklärung** der **Kinder über Risiken im Internet sind das A und O.** Zusätzlich können auch **technische Maßnahmen** helfen, das Erlebnis in der digitalen Welt möglichst sicher zu gestalten.

Prüfen Sie, ob auf dem von Ihren Kindern genutzten Endgerät alle wesentlichen **in Kapitel 1 genannten Grundlagen umgesetzt** sind.

Richten Sie für Ihr Kind ein eigenes **Benutzerkonto** mit **eingeschränkten Berechtigungen** ein und **konfigurieren** Sie dieses so, dass Ihr Kind nur Zugriff auf von Ihnen **freigeschaltete Anwendungen** hat.

Sie könnten auch **kindgerechte Suchmaschine hinterlegen** (z.B. Blinde Kuh) und ggf. Inhaltsfilter aktivieren**.**

Wenn **Smartphone oder Tablet** zum Lernen verwendet wird**,** installieren Sie **Apps nur aus vertrauenswürdigen Quellen** (App Store / Google Play).

Weitere umfangreiche Informationen und viele hilfreiche Websites zu dem Thema (z.B. Klicksafe oder Internet-ABC) finden Sie bei der Medienanstalt NRW.

Wie der Einsatz zu Hause gelingt

Wenn Ihre Kinder **Wissens-Apps, Lernplattformen oder Online-Spiele** nutzen, prüfen Sie anhand der folgenden **Kriterien** die **Qualität** der Angebot**:**

- Welche Institution steht hinter dem Angebot?
- Basiert das Angebot auf fundierten wissenschaftlichen Erkenntnissen?
- Sind die Inhalte kindgerecht aufbereitet?
- Sind die Inhalte frei von Werbung, In-App Käufen und Abos via SMS Aktivierung?
- Müssen Sie persönliche Daten angeben – und falls ja: Wofür werden diese genutzt?
- Falls es direkten Bezug auf die in der Schule behandelten Inhalte haben soll:

  Orientieren sich die Inhalte an den Lehrplänen der Bundesländer?

Halten Sie im Zweifel Rücksprache mit den Ansprechpartnern der Schule Ihres Kindes.

Cyber-Sicher durch die Krise – Kapitel 5

Klare Kommunikationswege

Für IT-Verantwortliche

Wenn ein Großteil der Kollegen ins Home-Office umzieht, ist die IT-Abteilung i.d.R. nicht mehr „über den Flur“ zu erreichen. Daher sollten umgehend klare Kommunikationswege und Ansprechpartner bestimmt werden – insbesondere für IT-Vorfälle.

CYBER SECURITY CLUSTER BONN

Konkrete Ansprechpartner für Mitarbeiter

Informieren Sie Ihre Mitarbeiter, welche Ansprechpartner in **IT-Support- und -Notfällen** zu kontaktieren sind und wie diese erreicht werden können.

Unser Tipp: Passen Sie die Vorlage (Download hier) an und erstellen Sie so eine Übersicht der Ansprechpartner für Ihre Mitarbeiter.

Falls Ihre IT durch **externe Dienstleister** betrieben wird, prüfen Sie deren aktuelle Erreichbarkeit.

Werden **personenbezogene Daten** entwendet, besteht ein **meldepflichtiger Vorfall**. Melden Sie solche Vorfälle umgehend. Informationen hierzu finden Sie auf der Website des BSI.

Cyber-Sicher durch die Krise – Kapitel 6

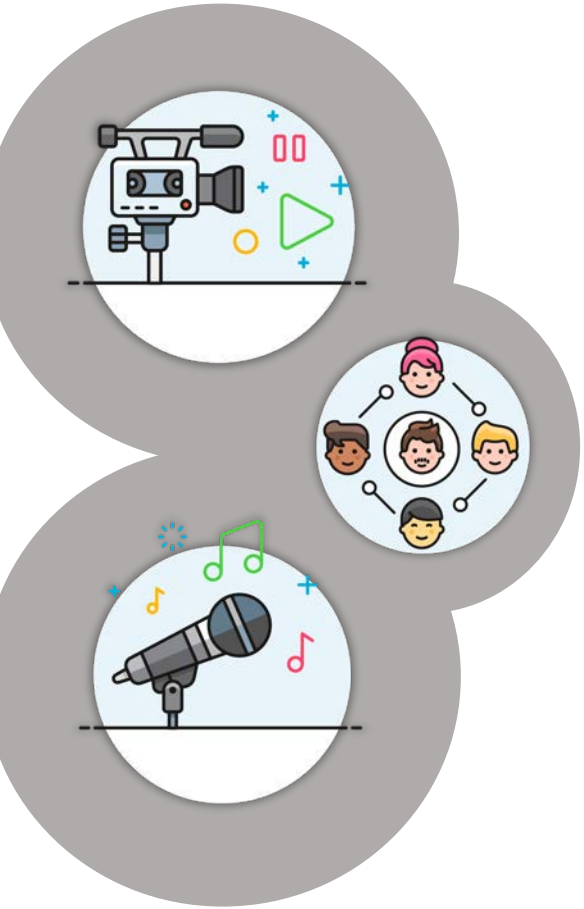
Videokonferenz Systeme

Für IT-Verantwortliche

Um mit dem Team und Kollegen in Kontakt zu bleiben, sind Videokonferenz Systeme derzeit oft die beste Möglichkeit. Im Folgenden vergleichen wir einige der häufig genutzten Systeme und erklären deren Vor- und Nachteile mit Fokus auf Aspekten des Datenschutzes und der Sicherheit.

CYBER SECURITY CLUSTER BONN

Vergleich häufig genutzter Tools



WebEx, Microsoft Teams, Zoom, GoToMeeting und Jitsi sind häufig verwendete **Video- und Webkonferenz-Tools.** Diese unterscheiden sich in Funktionalität, Preis sowie auch in Aspekten der IT-Sicherheit und des Datenschutzes.

Zur **Auswahl eines geeigneten Tools** empfehlen wir die Durchführung einer auf Ihr **spezifisches Anwendungsszenario** zugeschnittene **Risikoanalyse**.

Nutzen Sie den **nachfolgenden Aspekte** für Ihre Entscheidungsfindung:

- **Zugangsbeschränkungen:** Besprechungen sollten effektiv (durch Login, Passwörter etc.) vor unbefugter Teilnahme geschützt werden können. Dies ist bei allen auf der folgenden Seite aufgeführten Tools gegeben.
- **Blurr-Möglichkeit:** Zur Wahrung der Privatsphäre und zum Schutz sensibler Informationen kann es sinnvoll sein, den Hintergrund unkenntlich zu machen.
- **Regulierung von Aufnahmemöglichkeiten:** Wenn Tools die Möglichkeit einer Aufzeichnung bieten, so müssen alle Teilnehmer der Video-Konferenz deutlich auf die Aufzeichnung hingewiesen werden. Idealerweise wird die Einwilligung von den Teilnehmern automatisch abgefragt.
- **Standort des Anbieters und DSGVO-Konformität:** Es wird empfohlen, Lösungen von Anbietern zu verwenden, die in Deutschland oder innerhalb der EU Server betreiben.
- **Verschlüsselung:** Die Verschlüsselung der Datenübertragung findet bei Video-Telefonie auf verschiedenen Ebenen statt. Nähere Informationen hierzu finden Sie im BSI Kompendium zum Thema Videokonferenzsysteme.

Vergleich häufig genutzter Tools

WebEx (Cisco, USA)
Vorteile: viele Funktionen; kein Account und keine Installation für Teilnehmer der Konferenz notwendig; DSGVO leicht umsetzbar;
Nachteile: Blurr-Möglichkeit nur in iOS-App und in DeskPro Version;

Microsoft Teams (Microsoft, USA)
Vorteile: Universallösung für Zusammenarbeit inkl. Video-Konferenzen; sehr viele Funktionen; DSGVO leicht umsetzbar;
Nachteile: Anmeldung nur mit persönlichem Account; Einrichtung ohne Office 365-Abonnement zeitaufwendig; telefonische Einwahl nur per kostenpflichtigem Add-On;

Zoom (Zoom Video Communications, USA)
Vorteile: viele Funktionen; einfache Handhabung; kein Account und keine Installation für Teilnehmer an Konferenz notwendig;
Nachteile: Datenschutz-/Sicherheitsproblematik (Zoom reagiert darauf allerdings derzeit zügig)

GoToMeeting (LogMeIn, USA)
Vorteile: viele Funktionen; einfache Handhabung; kein Account und keine Installation für Teilnehmer an Konferenz notwendig; DSGVO leicht umsetzbar;
Nachteile: keine Blurr-Funktion;

Jitsi Meet (Open Source)
Vorteile: viele Funktionen; einfache Handhabung; auch für Initiator eines Meetings kein Account und keine Installation notwendig; kostenfrei;
Nachteile: ggf. Überlastung des Servers bei größerer Anzahl von Teilnehmern (auf Konfiguration achten); Aufnahme des Meetings nur via Dropbox und oft überlastet;

Cyber-Sicher durch die Krise – Kapitel 7

Sonstiges

Für IT-Verantwortliche

Weitere Empfehlungen finden Sie hier.

CYBER SECURITY CLUSTER BONN

Weitere Empfehlungen

Prüfen und beschränken Sie **Zugangsmöglichkeiten und Zugriffsrechte** auf Systeme und Informationen Ihrer Institution auf ein **notwendiges Mindestmaß**.

Stellen Sie **allgemeine Regeln** für die **Nutzung institutionsfremder IT-Systeme** auf.

Bieten Sie **übersichtliche Hinweise** für Mitarbeiter an, z.B. durch **kurze Anleitungen, Checklisten** oder **Videoschulungen**. Eine Checkliste für Mitarbeiter bietet z.B. die Allianz für Cybersicherheit des BSI. Auch eine Checkliste für IT-Verantwortliche steht hier zur Verfügung.

Anhang

CYBER SECURITY CLUSTER BONN

Quellenverzeichnis

Kapitel 1 – Allgemein Grundlagen

- https://de.m.wikihow.com/Die-Firmware-eines-Routers-aktualisieren
- https://www.pcwelt.de/ratgeber/WLAN-Router__Firmware-Update_Schritt_fuer_Schritt-Luecken_schliessen-8779421.html
- https://www.computerweekly.com/de/definition/Zwei-Faktor-Authentifizierung
- https://support.microsoft.com/de-de/help/12408/microsoft-account-how-to-use-two-step-verification
- https://www.fuer-gruender.de/blog/corona-homeoffice-it-sicherheit/
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.html
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf;jsessionid=58A343FC9CF1F1DE9F07A54FCB2A6169.2_cid369?__blob=publicationFile&v=9
- https://www.it-daily.net/it-sicherheit/cyber-defence/23761-so-arbeiten-mitarbeiter-sicher-im-home-office
- https://morethandigital.info/home-office-und-die-cyber-risiken/
- https://cyber-security-cluster.eu/de/aktuelles/sicher-home-office.html
- https://new.siemens.com/global/de/unternehmen/stories/forschung-technologien/cybersecurity/how-to-be-secure-in-the-home-office.html
- https://www.chip.de/news/USB-Stick-verschluesseln-So-gehts-kostenlos_145746855.html
- https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html
- https://workfromhome.education/de/home/

Kapitel 2 – Phishing / Spam-Mails / CEO-Fraud

- https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html
- https://www.ihk-niederbayern.de/nceo-fraud-betrueger-nehmen-verstaerkt-unternehmen-ins-visier-4533020
- https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Social_Engineering.html

Kapitel 3 – Gesund im Home-Office

- https://vanilla-mind.de/home-office-knigge/
- https://fitbase.de/homeoffice-so-bleiben-sie-gesund/
- https://www.dguv.de/de/mediencenter/pm/pressearchiv/2020/quartal_1/details_1_385472.jsp
- https://www.lia.nrw.de/themengebiete/Arbeitsschutz-und-Gesundheit/Homeoffice/index.html
- https://www.ispo.com/know-how/home-office-5-tipps-fuer-gesundes-arbeiten-daheim
- https://eatsmarter.de/gesund-leben/homeoffice-gesund-von-zu-hause-arbeiten
- https://www.dearemployee.de/gesund-im-home-office-in-zeiten-von-corona/
- https://www.bkk-mobil-oil.de/landingpages/homeoffice-tipps-corona.html

Quellenverzeichnis

Kapitel 4– Sicheres digitales Lernen zu Hause

- https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/tipps-fuer-eltern-sicher-digital-lernen.html
- https://www-de.scoyo.com/eltern/ratgeber/ratgeber-downloads/ratgeber-lernen-im-internet
- https://www.bitkom.org/Themen/Bildung-Arbeit/Anwendungen-digitaler-Unterricht
- https://www.gfdb.de/digitaler-unterricht/
- https://www.n-tv.de/panorama/Endlich-mehr-digitaler-Unterricht-article21654119.html
- https://bobblume.de/2020/03/23/digital-unterricht-digital-in-zeiten-vom-coronavirus/
- https://www.klicksafe.de/themen/schutzmassnahmen/jugendschutzfilter/

Kapitel 5 – Klare Kommunikationswege

- https://www.n-tv.de/technik/Vorsicht-Hacker-nutzen-Corona-Panik-article21636378.html
- https://www.stern.de/kultur/coronavirus-map--hacker-nutzen-unsicherheit-der-menschen-aus-9181812.html
- https://t3n.de/news/neue-angriffsvariante-1261675/
- https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/DigitaleDienste/Meldungen/meldungen_node.html

Kapitel 6 – Videokonferenz Systeme

- https://t3n.de/news/videokonferenz-software-im-vergleich-1265241/
- https://www.com-magazin.de/praxis/test/besten-web-konferenz-loesungen-im-test-1572086.html
- https://www.placetel.de/ratgeber/videokonferenzen
- https://www.computerwoche.de/a/die-wichtigsten-videokonferenz-systeme,3548602
- https://www.datenschutzbeauftragter-info.de/videokonferenz-tools-tipps-zur-auswahl-und-verwendung/

Kapitel 7 – Weitere Empfehlungen

- https://morethandigital.info/home-office-und-die-cyber-risiken/
- https://www.it-daily.net/it-sicherheit/cyber-defence/23761-so-arbeiten-mitarbeiter-sicher-im-home-office

Herausgeber, Danksagung und Disclaimer

Herausgeber
Dieses Dokument wurde vom Cyber Security Cluster Bonn e.V., Godesberger Allee 139, 53175 Bonn, erstellt und herausgegeben. Stand: 20. April 2020

Danksagung
Wir danken Stefan Becker vom Bundesamt für Sicherheit und Informationstechnik sowie Manuel Atug von der HiSolutions AG für ihr wertvolles Feedback, das in dieses Dokument eingeflossen ist.

Weitere Informationen zum Cyber Security Cluster Bonn e.V.

@CSCBonn **www.cyber-security-cluster.eu** **info@cyber-security-cluster.eu** **Clustermitglied werden**