



Folge 2: Von Homeoffices und Sprachassistenten

Unterschiede in den Locations

	Bisheriger Arbeitsplatz	Homeoffice	Maßnahmen im Homeoffice
Zugang zum Gebäude	<ul style="list-style-type: none"> ■ Token mit Zeitsteuerung ■ Gebäude alarmgesichert 	<ul style="list-style-type: none"> ■ Haustür mit normalem Schließzylinder. ■ Schlüssel bei der Putzhilfe, beim Nachbarn, beim Freund der Tochter ■ Besucher / Handwerker 	<ul style="list-style-type: none"> ■ Schlüsselausgabe überdenken
Zugang ins Büro	<ul style="list-style-type: none"> ■ Empfang ■ Besucherregelung 	<ul style="list-style-type: none"> ■ Zimmertür i.d.R. unverschlossen 	<ul style="list-style-type: none"> ■ Sensibilisierung
Gebäude-sicherheit	<ul style="list-style-type: none"> ■ Alarmsicherung ■ Pförtner ■ ggf. abgeklebte Fenster ■ sichere Verkabelung ■ etc. 	<ul style="list-style-type: none"> ■ Studenten-WG ■ Wohnung in Mehrfamilienhaus ■ Einfamilienhaus ■ Bildschirm evtl. von der Straße/Nachbarn einsehbar 	<ul style="list-style-type: none"> ■ Standort des Schreibtisches / Bildschirms / Telefons überdenken
Aufbewahrung von Informationen	<ul style="list-style-type: none"> ■ Im geschützten Büro ■ Aktenschrank ■ Safe ■ Tresor 	<ul style="list-style-type: none"> ■ Schublade, ■ Schreibtisch ■ da wo Platz ist 	<ul style="list-style-type: none"> ■ Ablage von Informationen überdenken ■ Clear Desk Policy sollte auch zu Hause gelten
Abhören	<ul style="list-style-type: none"> ■ Büro mit geregelter und durchdachter Absicherung 	<ul style="list-style-type: none"> ■ Büro in der Wohnung / Studenten-WG ■ Sprachassistenten (Alexa und Siri) in der Wohnung ■ Arbeiten auf der Terrasse (lautes sprechen) 	<ul style="list-style-type: none"> ■ Standort des Arbeitsplatzes überdenken ■ Sprachassistenten bei der Arbeit deaktivieren
Drucken	<ul style="list-style-type: none"> ■ Sicheres drucken mit PIN ■ PKI Karte ■ etc. 	<ul style="list-style-type: none"> ■ Unsicherer Drucker, evtl. im WLAN 	<ul style="list-style-type: none"> ■ Ausdrucken reduzieren, da ggf. auch eine sichere Vernichtung erforderlich ist ■ Standarddrucker ändern (um versehentliche sensible Ausdrücke im Büro zu vermeiden)

	Bisheriger Arbeitsplatz	Homeoffice	Maßnahmen im Homeoffice
Vernichten	<ul style="list-style-type: none"> ■ Aktenvernichter/ Dokumentenvernichter nach Vernichtungsklasse 	<ul style="list-style-type: none"> ■ Papierkorb ■ ggf. Low Budget Aktenvernichter/ Dokumentenvernichter 	<ul style="list-style-type: none"> ■ Wenig drucken ■ Darauf achten, was wie vernichtet werden muss!
Verwendung von Applikationen	<ul style="list-style-type: none"> ■ Company Applikationen, evtl. nur intern nutzbar 	<ul style="list-style-type: none"> ■ Nutzung von Workarounds oder RDP, um interne Ressourcen zu erreichen 	<ul style="list-style-type: none"> ■ Keine eigenen Workarounds (nur von der IT freigegebene) ■ Kein Umgehen der Unternehmensvorgaben ■ Keine privaten Dienste / Clouddienste nutzen
Kommunikation	<ul style="list-style-type: none"> ■ Eingespielte Abläufe per E-Mail ■ Festnetztelefon 	<ul style="list-style-type: none"> ■ Verstärkte Nutzung von Teams, Skype, Zoom, ... 	<ul style="list-style-type: none"> ■ Zunehmende Social Engineering Versuche per Telefon & E-Mail mit Bezug zu Remote Work oder Corona <p>Do's and don'ts in Webmeetings Beispiele:</p> <ul style="list-style-type: none"> ■ Meeting-URLs oder Zugangsdaten von virtuellen Sitzungen sind schützenswert ■ Serientermine die man einmalig weitergeleitet hat, können immer wieder verwendet werden. ■ Nicht über Social Media oder andere öffentliche Kanäle teilen (Siehe auch das negative Beispiel der EU-Sitzung der Verteidigungsminister).
Endgerät	<ul style="list-style-type: none"> ■ Verwaltung durch IT, sorgenfrei für den Mitarbeiter 	<ul style="list-style-type: none"> ■ Evtl. kein dauerhaftes Verwalten durch IT möglich? ■ VPN nicht dauerhaft eingeschaltet? ■ Ist im Einzelfall zu prüfen. 	<ul style="list-style-type: none"> ■ Bildschirm sperren ■ Auf Aktualität von Antivirus und Betriebssystem selbst achten.
Netzwerk	<ul style="list-style-type: none"> ■ Professionell administriertes Netzwerk 	<ul style="list-style-type: none"> ■ FritzBox, potenziell unsicheres WLAN. ■ Potenziell unsichere Router Konfigurationen (offenes WLAN, Standardkennwort im Router) 	<ul style="list-style-type: none"> ■ Auto-Update Funktion aktivieren ■ sicheres Kennwort ■ keine Standardkennworte unverändert nutzen