ISMS X-Plain
Informationssicherheit einfach erklärt

Folge 2:
Von Homeoffices und Sprachassistenten

Unterschiede in den Locations

	Bisheriger Arbeitsplatz	Homeoffice	Maßnahmen im Homeoffice
Zugang zum Gebäude	■ Token mit Zeitsteuerung ■ Gebäude alarmgesichert	■ Haustür mit normalem Schließzylinder. ■ Schlüssel bei der Putzhilfe, beim Nachbarn, beim Freund der Tochter ■ Besucher / Handwerker	■ Schlüsselausgabe überdenken
Zugang ins Büro	■ Empfang ■ Besucherregelung	■ Zimmertür i.d.R. unverschlossen	■ Sensibilisierung
Gebäude-sicherheit	■ Alarmsicherung ■ Pförtner ■ ggf. abgeklebte Fenster ■ sichere Verkabelung ■ etc.	■ Studenten-WG ■ Wohnung in Mehrfamilienhaus ■ Einfamilienhaus ■ Bildschirm evtl. von der Straße/Nachbarn einsehbar	■ Standort des Schreibtisches / Bildschirms / Telefons überdenken
Aufbewahrung von Informatio-nen	■ Im geschützten Büro ■ Aktenschrank ■ Safe ■ Tresor	■ Schublade, ■ Schreibtisch ■ da wo Platz ist	■ Ablage von Informationen überdenken ■ Clear Desk Policy sollte auch zu Hause gelten
Abhören	■ Büro mit geregelter und durchdachter Absicherung	■ Büro in der Wohnung / Studenten-WG ■ Sprachassistenten (Alexa und Siri) in der Wohnung ■ Arbeiten auf der Terrasse (lautes sprechen)	■ Standort des Arbeitsplatzes überdenken ■ Sprachassistenten bei der Arbeit deaktivieren
Drucken	■ Sicheres drucken mit PIN ■ PKI Karte ■ etc.	■ Unsicherer Drucker, evtl. im WLAN	■ Ausdrucken reduzieren, da ggf. auch eine sichere Vernichtung erforderlich ist ■ Standarddrucker ändern (um versehentliche sensible Ausdrucke im Büro zu vermeiden)

	Bisheriger Arbeitsplatz	Homeoffice	Maßnahmen im Homeoffice
Vernichten	■ Aktenvernichter/ Dokumentenvernichter nach Vernichtungsklasse	■ Papierkorb ■ ggf. Low Budget Aktenvernichter/ Dokumentenvernichter	■ Wenig drucken ■ Darauf achten, was wie vernichtet werden muss!
Verwendung von Applikationen	■ Company Applikationen, evtl. nur intern nutzbar	■ Nutzung von Workarounds oder RDP, um interne Ressourcen zu erreichen	■ Keine eigenen Workarounds (nur von der IT freigegebene) ■ Kein Umgehen der Unternehmensvorgaben ■ Keine privaten Dienste / Clouddienste nutzen
Kommunikation	■ Eingespielte Abläufe per E-Mail ■ Festnetztelefon	■ Verstärkte Nutzung von Teams, Skype, Zoom, ...	■ Zunehmende Social Engineering Versuche per Telefon & E-Mail mit Bezug zu Remote Work oder Corona Do's and don'ts in Webmeetings Beispiele: ■ 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	■ Verwaltung durch IT, sorgenfrei für den Mitarbeiter	■ Evtl. kein dauerhaftes Verwalten durch IT möglich? ■ VPN nicht dauerhaft eingeschaltet? ■ Ist im Einzelfall zu prüfen.	■ Bildschirm sperren ■ Auf Aktualität von Antivirus und Betriebssystem selbst achten.
Netzwerk	■ Professionell administriertes Netzwerk	■ FritzBox, potenziell unsicheres WLAN. ■ Potenziell unsichere Router Konfigurationen (offenes WLAN, Standardkennwort im Router)	■ Auto-Update Funktion aktivieren ■ sicheres Kennwort ■ keine Standardkennworte unverändert nutzen