ISMS X-Plain

Informationssicherheit einfach erklärt

Folge 2:
Von Homeoffices und Sprachassistenten

Maßnahmen in der IT

#1 Computer aus Firma nach HomeOffice transportiert?

Haben Sie einige Ihrer Mitarbeiter mit Computern ausgestattet, die bislang nie außerhalb Ihres lokalen Netzwerks waren? Stellen Sie sicher, dass sie gepatcht und in Ihren Endgeräte-Schutz integriert sind.

#2 Company PCs immer noch gemanaged?

Sehen Sie diese Geräte in der Konsole Ihres zentralisierten Endpoint Protection?
Sehen Sie wirklich alle?

#3 Welche Daten im HomeOffice? Verschlüsselung?

Welche Art von Daten haben Ihre Mitarbeiter mitgenommen?
Überprüfen Sie, ob die Notebooks verschlüsselt sind.

#4 Überprüfe VPN-Konfig

Haben Sie gerade eine neue VPN-Box zwischen Internet und dem lokalen Netzwerk installiert?
Stellen Sie sicher, dass Sie die aktuellste Firmware installiert haben.

#5 Überprüfe Firewall-Konfig

Mussten Sie neue Firewall-Regeln konfigurieren? Handelt es sich um eine any-any-Richtlinie, die jedem Remote Device vollen Zugriff auf Ihr Unternehmensnetzwerk erlaubt? Prüfen Sie, ob dies wirklich erforderlich ist.

#6 Überprüfe Zugangsdaten

Haben Sie ein einzelnes Konto in der Form „Name:VPN“ und „Passwort:Firma“ für den Verbindungsaufbau über VPN konfiguriert, weil Sie wissen, dass Ihre internen Ressourcen ohnehin eine zweite Authentifizierung gegen das Active Directory benötigen?
Stellen Sie sicher, dass jeder Einzelne seine personalisierten Zugangsdaten erhält.

#7 Multi Faktor Anmeldung aktiviert!

Ist die Multi-Faktor-Authentifizierung aktiviert?
Es ist eine gute Idee, MFA zu implementieren. Besonders wenn starke Passwörter nicht erzwungen werden.

#8 Nur sichere Verbindungen

Haben Sie berücksichtigt, dass den Netzwerken zwischen dem Telearbeit-Client und Ihrem Unternehmensnetz nicht vertraut werden kann? Da zählt auch das private WLAN-Netz des Mitarbeiters dazu.
Der Einsatz von Verschlüsselungstechnologien zum Schutz der Vertraulichkeit und Integrität der Kommunikation ist ein Muss. Sogar in Situationen wie dieser.

#9 Windows XP / Windows 7 im Home-Office-Netz oder Prüfung, wer ins Company Netz darf

Haben Sie sichergestellt, dass keine alten Kisten mit Windows XP oder Windows 7 an Ihr Netzwerk angeschlossen sind?
Stellen Sie sicher, dass diese isoliert sind und mit einem separaten Netzwerk verbunden sind, das für externe Client-Geräte bestimmt ist.

#10 Welche Geräte dürfen sich am VPN anmelden?

Haben Sie sichergestellt, dass sich nur Company Geräte in Ihrem Netzwerk anmelden dürfen.

#11 Der andere Weg: interne oder unsichere Systeme ins Internet gebracht (z.B. RDP)? Prüfen!

Haben Sie einfachheitshalber interne Systeme ins Internet gebracht? Dies wurde vorher vielleicht nie in Betracht gezogen.
Stellen Sie sicher, dass die Systeme, die vom Internet aus erreichbar sind, gehärtet und der Zugriff auf ein Minimum beschränkt ist.

#12 Kapazitäten und Logfiles überwachen