ADDVISIONS ONEPAGER OM SIKKERHED

DU VED, AT DET KUN ER ET SPØRGSMÅL OM TID – KORT TID – FØR DIN VIRKSOMHED BLIVER ANGREBET AF CYBERKRIMINELLE. HACKING. RANSOMWARE. DATANEDBRUD. ELLER NOGET FJERDE.

HER FÅR DU ADDVISIONS KORTE OG OVERSKUELIGE TJEKLISTE OM DIGITAL BASIS-SIKKERHED.

FØLGER DU RÅDENE, NEDSÆTTER DU DIN RISIKO FOR AT ANGREBET LYKKES MED 90%.

3-2-1 REGLEN VED BACKUP

Backup er det vigtigste, du kan gøre. Har du ikke backup, kan du ikke genskabe data. Uanset om det er hackere eller force majeure. 3-2-1 betyder, at du har 3 backups. 2 af sikkerhedskopierne skal være på forskellige lagringsmedier (fx skyen og eksternt medie), og 1 af sikkerhedskopierne skal være placeret et andet fysisk sted. Er du endnu mere hardcore, kan du bruge 3-2-2 reglen, hvor du har 2 x 2 kopier på forskellige medier og forskellige fysiske adresser. Tag din backup ofte, helst hver dag.

2-FAKTOR GODKENDELSE OG REGLER FOR KODEORD

Der er ingen undskyldning for ikke at have 2-faktor godkendelse overalt i dag. Ideelt set kobler du det med automatisk genererede kodeord. Beskyt allerede din Office 365 ved at aktivere det som du kan gøre her: https://aka.ms/mfasetup

RETTIGHEDSSTYRING FOR LOKALE ADMINISTRATORER

Lad kun IT-afdelingen eller den IT-ansvarlige installere på servere og arbejdsstationer. Er det upraktisk, så indfør rettighedsstyring med godkendelse, så lokale administratorer/brugere intet kan installere uden en digital godkendelse fra IT-afdelingen.

AUTOMATISK OPDATERING AF PROGRAMMER OG SYSTEMER

Sørg for at samtlige systemer og programmer er indstillet til automatisk opdatering. På den måde får du lukket huller og alle de sikkerhedsforanstaltninger, som dygtige udviklere løbende tilfører deres software.

HJEMMEARBEJDE

Der er større risiko for sikkerhedsbrud ved hjemmearbejde end på arbejdspladsen. Brug kun computere og kommunikationskanaler, som er godkendt af virksomheden, til hjemmearbejde. Lad aldrig andre få adgang til computeren.

FIREWALL OG ANTIVIRUS

En firewall blokerer udvalgte programmer og programtyper fra at få adgang til virksomhedens systemer og netværk. Antivirus scanner og patruljerer løbende systemer og programmer på samtlige virksomhedens enheder. Det er standard, når du får hostet virksomhedens IT, og du må aldrig nogensinde vælge det fra, hvis du selv har systemer, programmer og data liggende.

LOKAL SERVER VS HOSTING

Medmindre du er verdens skarpeste teknolog, så får du større sikkerhed, når din virksomheds systemer og data er hostede, frem for at du selv håndterer det. Mere er der ikke at sige om det.

FYSISK SIKKERHED

Du skal have styr på den digitale sikkerhed – men glem ikke ganske almindelige indbrud, hvor computere og lignende kan blive stjålet. Vær ikke nærig med alarmsystemet, og lås også kontorer, skabe osv. efter arbejdstid.

PHISHING

Lad være at klikke. Lad være at svare. Udlevér ikke oplysninger. Tjek ikke bare én gang, men 2-3 gange. Lad nu bare være!

KAN DU SELV? VIRKELIG?
ELLER ER DU SIKRERE, HVIS DU FÅR EKSTERN HJÆLP?

Er digital sikkerhed din kernekompetence? Hvis ikke, så overvej at købe hosting og sikkerhed på abonnement. Vi (eller de) er dygtige, uddannede og konstant opdaterede på området.
Slip tøjlerne, bliv meget mere sikker, og koncentrér dig om dét, du er god til.

Få et gratis og uforpligtende møde med os.
Vi har 30 års erfaring med alt vedrørende IT og rådgiver dig i øjenhøjde.
Klik her og bed om dit gratis møde

ADDVISION
KOMPLETTE IT-LØSNINGER

ADDvision a/s, Kantatevej 26B, 2730 Herlev - +45 44 53 03 33 - info@addvision.dk - addvision.dk