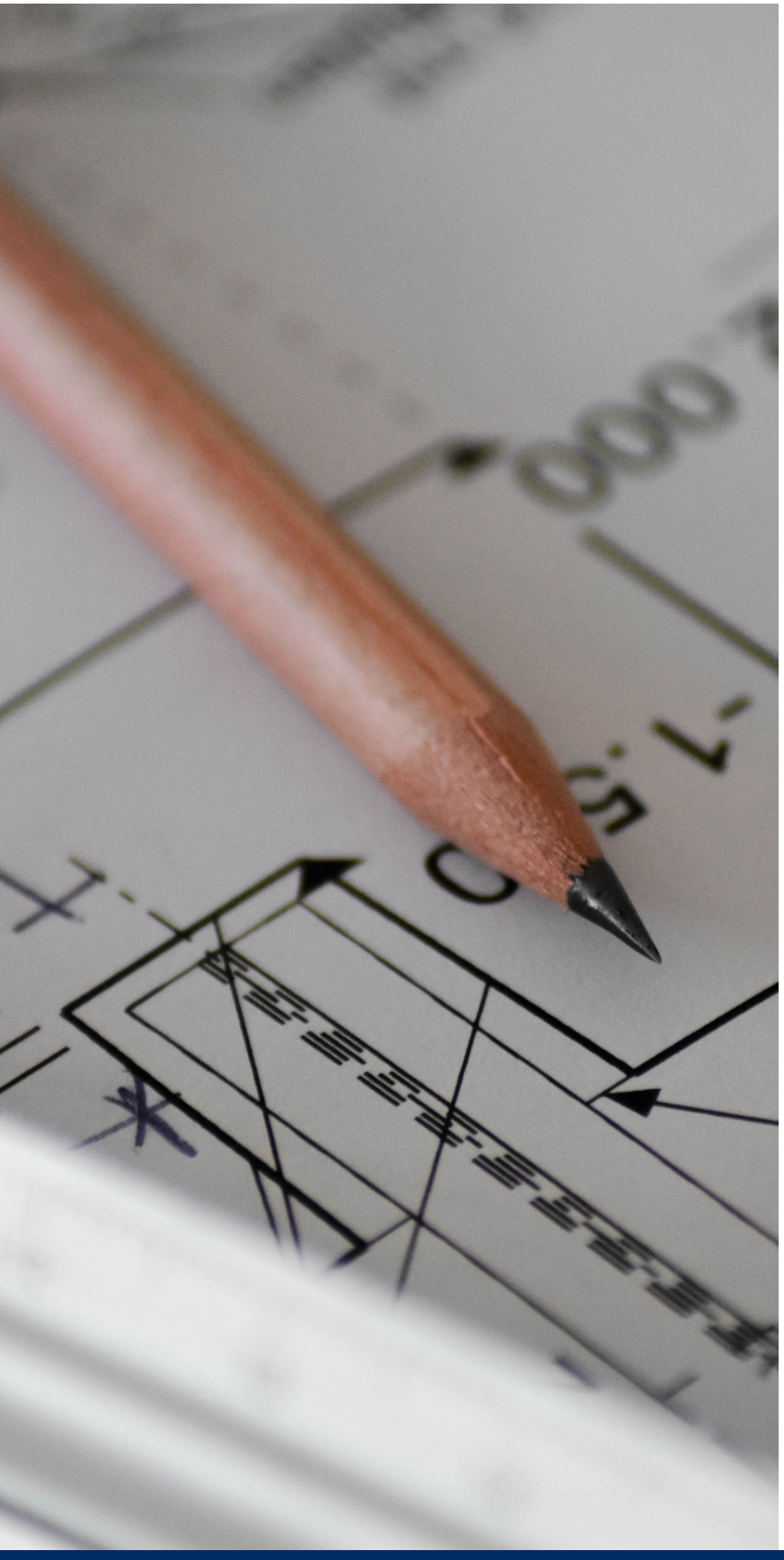
Dansk IT Sikkerhed

SIKRING AF DIGITALE FUNDAMENTER 2023

EN OMFATTENDE ANALYSE AF CYBERSIKKERHEDSPRAKSIS I BYGGE- OG ANLÆGSSEKTOREN

INDHOLD



AT NAVIGERE IND I FREMTIDEN

Bygge- og anlægssektoren begivet sig ud på en transformationsrejse, hvor man omfavner banebrydende teknologier for at optimere drift, forbedre effektivitet og fremme innovation. Men i takt med at sektoren bevæger sig ind i digital transformation, står den også over for en eskalerende række af cybertrusler, der har potentiale til at kompromittere følsomme data, forstyrre projektplaner og undergrave tilliden indenfor industrien.

Denne rapport dykker ned i oversete detailjer omkring cybersikkerhedspraksis inden for bygge- og anlægssektoren. Ved at trække indsigt fra en detaljeret markedsundersøgelse foretaget blandt en mangfoldig vifte af bygge- og anlægsvirksomheder søger denne rapport at afsløre de sammenflettede forhold mellem forskellige cybersikkerhedsforanstaltninger.

Gennem denne udforskning har vi til hensigt at give byggeorganisationer viden til at navigere i skæringspunktet mellem teknologisk udvikling og robust cybersikkerhed.

CLAUS ELNEGAARD HANSEN
FORMAND

BYGGERI I ET DIGITALT LANDSKAB

AF DKITS

Bygge- og anlægssektoren, kendt for at opføre fysiske strukturer, er nu også engageret i at konstruere sit digitale landskab. Ved at omfavne Building Information Modeling (BIM), Internet of Things (IoT) enheder til overvågning af byggepladser og cloudbaserede projektstyringsplatforme til forbindelse af forskellige byggefirmaer og teams, forbedrer kommunikationen og strømliner processer som aldrig før. Men denne hurtige digitale integration udsætter også sektoren for hidtil usete sårbarheder.

Denne rapport undersøger ti forskellige cybersikkerhedspraksis og gransker deres betydning og samspil inden for bygge- og anlægssektoren.

"IT i bygge- og anlægsbranchen er i dag lige så nødvendigt som konventionelt værktøj."

Hver praksis, fra håndtering af adgangskoder til respons på kunstig intelligens (AI) trusler, repræsenterer en unik facet af sektorens udviklende cybersikkerhedslandskab. Denne undersøgelse er baseret på en rundspørge blandt 1360 danske SMV'er i bygge- og anlægsbranchen, undersøgelsen indeholder også få tal fra en tidligere tværfaglig undersøgelse udført at Dansk IT Sikkerhed i Q2 2023. Hele procenttal kan være rundet til nærmeste hele tal. Vi tager forbehold for regne og tastefejl i denne rapport.

ANVENDELSE AF SMART VÆRKTØJ I DANMARK

9,5%

Af de danske byggefirmaer har omfavnet muligheden for at anvende internetopkoblet værktøj.

90,5%

Størstedelen er stadig ikke intresseret i at benytte sig af de nye muligheder for digitalt udstyr.

BRUG AF SMART VÆRKTØJ

Med 130 respondenter, der svarer "Ja" og 1230 respondenter, der svarer "Nej", er det tydeligt, at en betydelig del af den undersøgte population ikke bruger IoT-værktøjer dagligt.

Undersøgelsesresultaterne understreger, at en betydelig majoritet af respondenterne ikke engagerer sig med IoT-enheder på daglig basis. Dette kan indikere tøven eller begrænset integration af IoT-værktøjer i deres rutiner.

Da IoT-enheder bliver stadig mere almindelige, kan kløften mellem implementering og sikkerhedsbevidsthed skabe sårbarheder. Mange IoT-enheder har været mål for cyberangreb på grund af utilstrækkelige sikkerhedsforanstaltninger. Den lave daglige brug kan afspejle en bevidst indsats for at mindske potentielle risici forbundet med disse enheder.

Kontrasten mellem virksomheder der har valgt at bruge disse nye digitale værtøjer og dem der ikke har antyder, at mens IoT-teknologi vinder frem, er den endnu ikke blevet udbredt. Dette kan tilskrives faktorer som enhedsomkostninger, begrænset kendskab til tilgængelige applikationer eller bekymringer om datasikkerhed og -privatliv.

HVOR STÅR VI I DAG?

Det lave antal brugere kan indikere tekniske forbehold forbundet med IoT-enheder. Organisationer må anerkende disse bekymringer og imødegå dem proaktivt ved at forbedre enhedssikkerhedsfunktioner og levere klare privatlivskontroller.

På baggrund af kløften i forhold til implementeringen er der en mulighed for at uddanne brugere om fordelene ved IoT-enheder og måder at bruge dem sikkert på. At fremme bedste praksisser såsom regelmæssige softwareopdateringer og stærk adgangskodehåndtering kan fremme sikrere brug.

Organisationer, der udvikler IoT-enheder, bør prioritere robuste privatlivsbeskyttelser, der sikrer, at brugerdata indsamles, behandles og opbevares i overensstemmelse med relevante regulativer. Dette kan hjælpe med at mindske privatlivsbekymringer og fremme bredere

Producenter af IoT-enheder bør implementere sikkerhedsforanstaltninger på hvert udviklingsstadie, herunder hardware, software og kommunikationsprotokoller. Sikkerhed skal være en integreret del af designprocessen snarere end en eftertanke.

Forenklede og intuitive brugergrænseflader kan fremme bredere implementering blandt ikke-tekniske brugere. Enheder, der er nemme at opsætte, konfigurere og administrere, kan udfylde kløften mellem daglige brugere og ikke-brugere.

Producenter bør kommunikere deres politikker for dataindsamling og -anvendelse gennemsigtigt til brugerne. At opbygge tillid ved at være åben om, hvordan data håndteres, kan hjælpe med at mindske bekymringer og øge populariteten.

Forskellen mellem daglige brugere og ikke-brugere af IoT-værktøjer belyser et komplekst landskab, hvor sikkerhedsbekymringer, markedsmodenhed og bevidsthed krydser hinanden.

ANVENDELSE AF KRYPTERET BACKUP

24,3%

Af de danske byggefirmaer har sørget for at få opsat en GDPR compliant krypteret backup løsning.

75,7%

Størstedelen har stadig i ikke set behovet for at kryptere og sikre deres kundedata, regnskaber, mv.

RANSOMWARE TRUER BYGGERIET

I byggebranchen har under en fjerdedel af virksomhederne valgt at sikre deres IT udstyr og data med en krypteret backup.

Et tal der ligger langt under det tværfaglige gennemsnit blandt danske virksomheder af samme størelse (47%), en bekymrende og opsigtvækkende konstatering og muligtvis den vigtigste udfordring for industrien at addresere.

"I 2022 blev over 1600 danske virksomheder ramt af ransomware, kun 65% fik deres data tilbage."

Data indikerer, at en betydelig majoritet af respondenterne ikke anvender krypterede backups. Dette rejser spørgsmål om datasikkerhed og graden af bevidsthed om vigtigheden af at kryptere backup-data.

Uden kryptering er backup-data sårbart over for uautoriseret adgang, hvis backup-filerne falder i de forkerte hænder. Denne situation kan føre til datalækager, hvor følsomme oplysninger kompromitteres.

Det store antal respondenter, der ikke bruger krypterede backups, kan afspejle en mangel på bevidsthed om de potentielle risici og fordele, der er forbundet med denne praksis. Organisationer og enkeltpersoner kan undervurdere værdien af kryptering i beskyttelsen af data.

STRATEGIER FOR FORBEDRINGER

Organisationer såvel som enkeltpersoner bør implementere en politik om at kryptere alle backups som en standard praksis. Dette sikrer, at data forbliver beskyttede, selv i tilfælde af tab, tyveri eller kompromittering af de fysiske backup-medier.

Det er af afgørende betydning at højne bevidstheden om vigtigheden af krypterede backups. Organisationer bør tilbyde træning til deres medarbejdere og brugere om de risici, der er forbundet med ubeskyttet backup-data, og hvordan kryptering kan reducere disse risici.

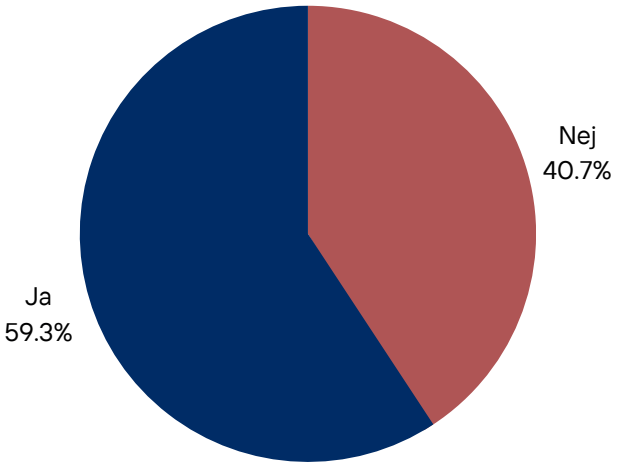
Backup-løsninger bør inkludere automatiserede krypteringsmekanismer for at gøre processen mere brugervenlig. Dette mindsker byrden ved manuelt at implementere kryptering og øger sandsynligheden for at opretholde sikre praksisser.

Regelmæssig testning af backup- og gendannelsesprocessen er af afgørende betydning. Dette inkluderer at sikre, at krypterede backups kan gendannes med succes for at mindske risikoen for datatab på grund af tekniske fejl.

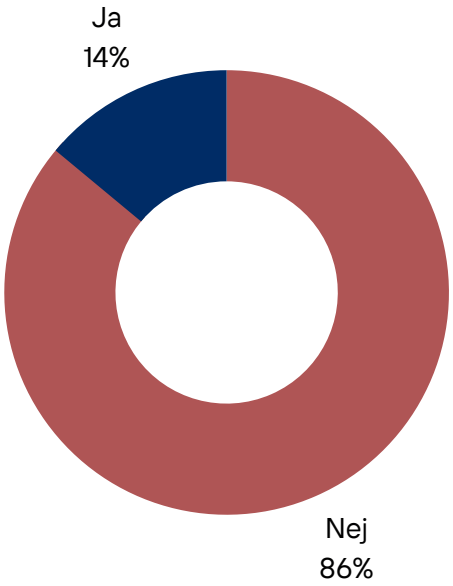
Dataens afsløring af en bemærkelsesværdig kløft i anvendelsen af krypterede backups understreger behovet for øget fokus på sikkerhed og praktisk implementering. At fremhæve vigtigheden af kryptering af backup-data kan bidrage væsentligt til at beskytte følsomme oplysninger og reducere risikoen for datalækager. Krypterede backups beskytter ikke kun mod eksterne trusler, men spiller også en vital rolle i at håndtere potentielle insidertrusler og sikre overholdelse af regler. I takt med at det digitale landskab udvikler sig, er det afgørende at integrere kryptering som en grundlæggende del af backup-strategierne for at forbedre den samlede cybersikkerhedsposition.

ADGANGS KONTROL I BYGGERIET

Anvender virksomheden altid 2-faktor godkendelse?



Anvender virksomheden Password Management?



Det er opmuntrende at se, at et flertal af virksomhederne (59.3%) har implementeret to-faktor godkendelse som en ekstra lag af sikkerhed. Dette er en vigtig foranstaltning for at beskytte adgangen til vigtige systemer og data.

På trods af de positive resultater er der stadig en betydelig andel af virksomheder (40.7%) der ikke anvender 2FA. Dette udgør en potentielt høj risiko, da en enkelt faktor (normalt en adgangskode) ikke altid er tilstrækkelig til at forhindre uautoriseret adgang.

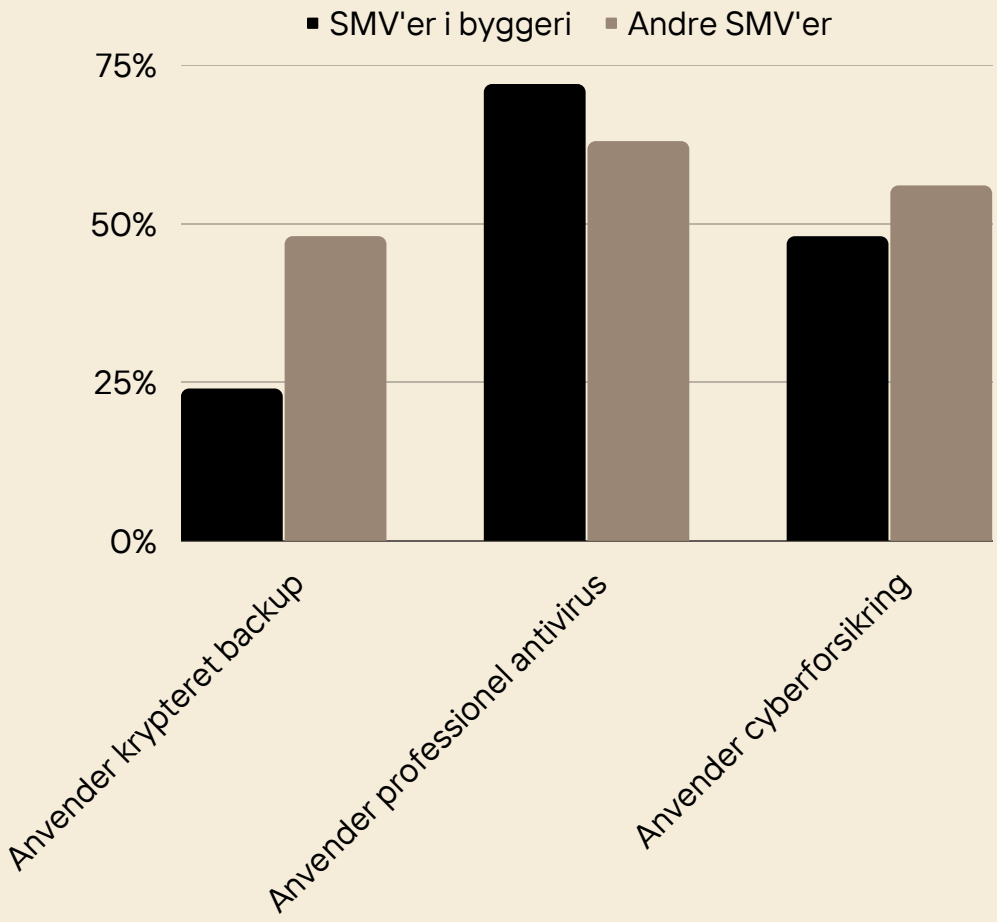
Virksomheder, der ikke anvender 2FA, er mere sårbare over for adgangsrelaterede trusler som f.eks. phishing-angreb eller adgangskode-lækager. En enkelt adgangskode kan nemt blive kompromitteret, hvilket kan føre til uautoriseret adgang til følsomme oplysninger.

Det er bemærkelsesværdigt, at en overvældende majoritet af virksomheder (86%) ikke anvender password managers. Dette antyder, at der er et betydeligt behov for at forbedre sikkerheden omkring adgangskoder i disse virksomheder.

Manglen på brug af password managers kan resultere i mangel på dækning fra cyberforsikring, som er en betydelig sikkerhedsrisiko.

Kombinationen af at 48% af de adspurgte anvender cyberforsikring, men kun 14% lever op til en af de ofte standardiserede krav for dækning af denne forsikring er et udtryk for manglende oplysning omkring IT-sikring og sikkerhed i branchen.

Uden brug af password managers er der en større risiko for, at medarbejdere opretter svage adgangskoder, genbruger adgangskoder på tværs af tjenester og ikke opdaterer dem regelmæssigt.



SAMMENLIGNING

Her sammenligner vi SMV'er (Små og Mellemstore Virksomheder) i byggebranchen med SMV'er i andre sektorer vedrørende deres brug af krypteret backup, anvendelse af professionel antivirus og dækning med cyberforsikring.

24% af SMV'erne i byggebranchen anvender krypteret backup, mens 48% af SMV'erne i andre sektorer gør det. Dette indikerer, at SMV'er i byggebranchen gør mindre brug af krypteret backup sammenlignet med SMV'er i andre industrier.

SMV'er i byggebranchen har en udfordring med lav implementation af krypteret backup, hvilket kan øge deres risiko for datatab i tilfælde af uautoriseret adgang eller tekniske problemer.

Manglende data kryptering kan føre til bøder og henstillinger fra datatilsynet, her er virksomhederne i byggebranchen betydeligt mere udsat end gennemsnittet af andre brancher. SMV'er i byggebranchen bør overveje at oplyse og promoverer brugen af krypteret backup for at forbedre deres datalagrings-sikkerhed.

På den positive side har SMV'er i byggebranchen en højere ratio af brugere af professionel antivirus, hvilket er afgørende for at beskytte sig mod malware og andre trusler. 72% af SMV'erne i byggebranchen bruger professionel antivirus, mens 63% af SMV'erne i andre sektorer gør det.

48% af SMV'erne i byggebranchen er dækket med cyberforsikring, sammenlignet med 56% af SMV'erne i andre sektorer. Selvom dækningen med cyberforsikring er lidt lavere i byggebranchen, er det stadig vigtigt for SMV'er at overveje, da det kan hjælpe med at dække omkostningerne ved datalækager eller cyberangreb.

Både byggeriet og de andre SMV'er i DKITS seneste 2 undersøgelser indikerer dog desværre stadig en stor eksponering i det danske erhvervsliv overfor hackere.

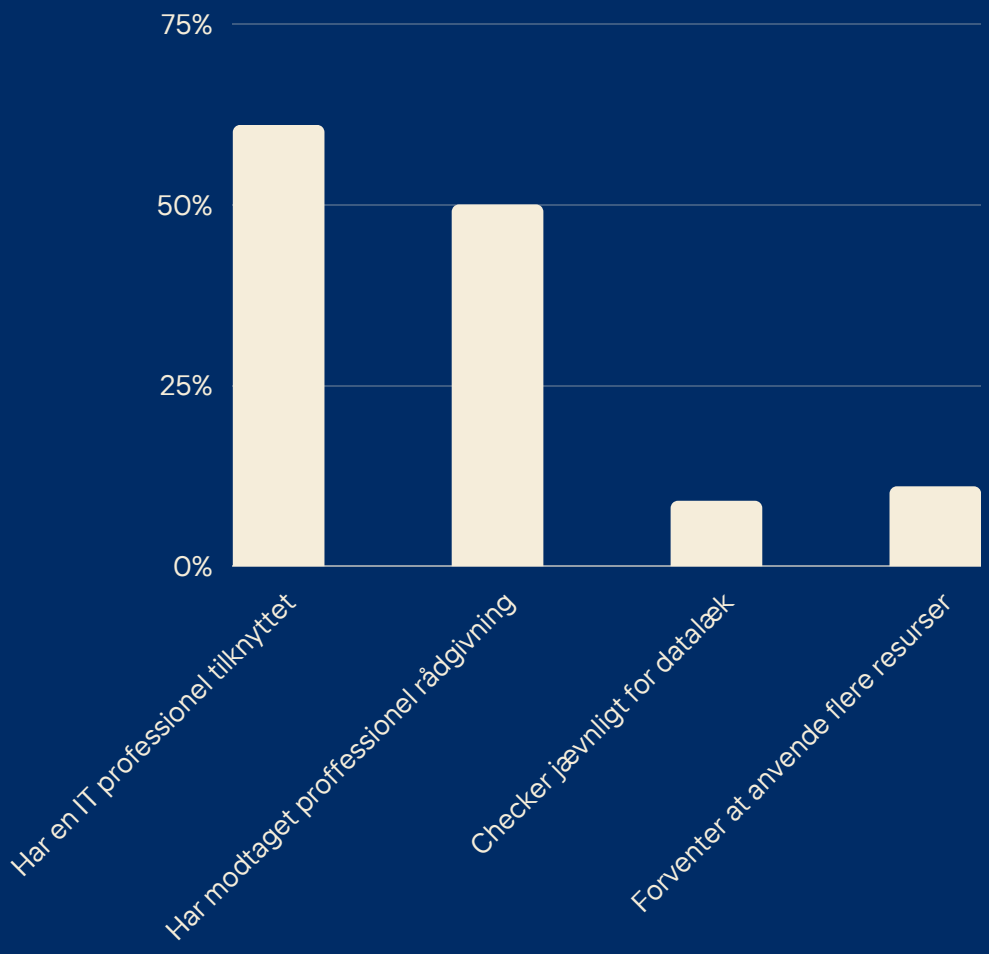
KUNSTIG INTELLIGENS SOM EN TRUSSEL

15,6%

Af de danske byggefirmaer ser AI og kunstig intelligens som en valid trussel imod den danske datasikkerhed.

84,4%

Af håndværkerne ser ikke kunstig intelligens som en relevant faktor i sikkerheden af IT-Systemer.



ENGAGEMENT

Her ser vi nærmere på hvor bred en forståelse og hvor stort et engagement den danske byggebranche har, i at forstå, forbygge og følge op på datalæk i samspil med IT-Udbyderne.

Den præsenterede data giver os et fascinerende indblik i, hvordan danske bygge- og anlægsvirksomheder forholder sig til spørgsmål om datalæk og deres interaktion med IT-udbydere. Disse tal tegner et billede af både styrker og svagheder inden for sektoren, når det kommer til at tackle den stigende trussel mod datasikkerhed og privatliv.

Over 60% af virksomhederne rapporterer, at de har en IT-professionel tilknyttet deres organisation. Dette er en positiv indikation af, at mange virksomheder er opmærksomme på vigtigheden af at have teknisk ekspertise i huset. IT-eksperter spiller en afgørende rolle i udviklingen og implementeringen af effektive sikkerhedsforanstaltninger, der kan beskytte mod datalæk og cyberangreb.

Halvdelen af virksomhederne har søgt professionel rådgivning om cybersikkerhed og datalæk. Dette vidner om en proaktiv tilgang til at forbedre sikkerhedspraksis.

Samarbejdet med eksterne eksperter kan bidrage til at identificere potentielle trusler og svagheder, som virksomhederne måske ikke selv har opdaget.

En udfordrende observation er, at kun 9% af virksomhederne rapporterer, at de regelmæssigt kontrollerer for datalæk. Dette er en væsentlig bekymring, da det tyder på, at mange virksomheder ikke er proaktive nok med hensyn til at opdage og forhindre datalæk i deres systemer. Dette kan potentielt føre til betydelige sikkerhedsrisici og tab af fortrolig information.

Cirka 11% af virksomhederne forventer at øge deres ressourcer og investeringer i cybersikkerhed og datalæk i fremtiden. Dette kan indikere, at der er en voksende bevidsthed om den eskalerende trussel, som datalæk udgør. Virksomheder erkender behovet for at styrke deres sikkerhedsinfrastruktur for at beskytte deres digitale aktiver og følsomme data.

ER BYGGERIET I FARE?

Selvom der er positive træk i form af tilknytning af IT-professionelle og søgen efter professionel rådgivning inden for cybersikkerhed, er der stadig betydelige udfordringer i form af manglende regelmæssig kontrol for datalæk. Dette er et område, hvor virksomhederne bør fokusere på at forbedre deres praksis.

Der er en klar anerkendelse af behovet for øgede investeringer i cybersikkerhed, men det er vigtigt, at denne bevidsthed følges op med konkrete handlinger. Virksomheder bør arbejde på at etablere en kultur, der prioriterer regelmæssig overvågning, risikostyring og vedvarende forbedring af deres sikkerhedsforanstaltninger.

Datalæk er en alvorlig trussel, der kan have ødelæggende konsekvenser for en virksomheds omdømme og økonomi. Det er afgørende for danske bygge- og anlægsvirksomheder at træffe de nødvendige foranstaltninger for at beskytte deres digitale aktiver og forblive i forkant med de stadig mere avancerede cybertrusler. Det indebærer en kombination af teknologi, uddannelse og en forpligtelse til konstant at forbedre sikkerheden.

OVERBLIK AF TILSTANDEN

I denne raport har vi udforsket en bred vifte af emner inden for cybersikkerhed og datalæk i konteksten af danske bygge- og anlægsvirksomheder. Vi har analyseret data fra en omfattende markedsundersøgelse og trukket værdifulde indsigter, der afspejler både udfordringer og muligheder i en tid, hvor digitalisering og teknologiske fremskridt er i konstant udvikling i denne sektor.

Vores analyse begyndte med at undersøge, hvordan danske bygge- og anlægsvirksomheder ser på cybersikkerhed. Resultaterne fremhævede behovet for øget fokus på dette område, hvor kun et mindretal havde indført stærke sikkerhedsforanstaltninger som brugen af password managers, krypteret backup og regelmæssig kontrol for datalæk.

Fra potentielle datalæk til den stigende trussel fra kunstig intelligens, har vores analyse belyst, hvor vigtigt det er for virksomheder at være proaktive og i stand til at tilpasse sig det skiftende trussellandskab.

For at hjælpe danske bygge- og anlægsvirksomheder med at styrke deres cybersikkerhedsforanstaltninger, har vi identificeret en række strategier for forbedring.

Det er ikke længere tilstrækkeligt at reagere på trusler, når de opstår; proaktivitet og forebyggelse er nøglen til at minimere risici og beskytte virksomhedens omdømme og økonomiske stabilitet. I en verden, der konstant udvikler sig teknologisk, er cybersikkerhed en dynamisk disciplin. Virksomheder skal forblive agile og indstillet på at tilpasse deres sikkerhedsstrategier i takt med nye trusler og muligheder.

"Brugernes adfærd, uddannelse og bevidsthed spiller en afgørende rolle i at beskytte organisationers digitale aktiver."

Den danske bygge- og anlægssektor står over for udfordringer og muligheder inden for cybersikkerhed, og vores mål med denne rapport er at give en dybdegående forståelse af landskabet og de skridt, der kan tages for at forbedre sikkerheden. Vi håber, at de indsigter og anbefalinger, der er præsenteret her, vil tjene som et værdifuldt redskab for virksomheder, beslutningstagere og alle, der er engageret i at beskytte danske bygge- og anlægsvirksomheder mod de voksende trusler inden for cybersikkerhed. Sammen kan vi arbejde mod en mere sikker digital fremtid.

91%

Af de danske bygge- og anlægvirksomheder tjekker ikke DarkWeb for tab af data, personoplysninger eller login-oplysninger.

28%

Af de danske bygge- og anlægvirksomheder har ikke installeret et basalt anti-virus program på deres digitale enheder i midten af 2023.

78%

Af de danske bygge- og anlægvirksomheder har endnu ikke set behovet for password managment, hvilket er et krav for dækning af cyberforsikring.

89%

Af de danske bygge- og anlægvirksomheder mener ikke det bliver nødvendigt at investere yderligere i digital sikkerhed i det kommende år.

DANSK IT SIKKERHED
HJORTLUNDVEJ 16
6771 GREDSTEDBRO
CVR 43285726
INFO@DKITS.DK
BESØG OS PÅ DKITS.DK