

CON
TECH
LAB_

An aerial photograph of a construction site, showing various materials, workers, and equipment. Overlaid on the image are several semi-transparent blue circular and rectangular patterns, suggesting digital data or security protocols. A large, stylized blue padlock icon is positioned in the lower-left quadrant of the image, partially overlapping the construction site. The overall theme is the integration of digital technology and security in the construction industry.

Sikkert Digitalt Samarbejde i byggeriet

0.0

Kolofon

Denne publikation er udgivet af **ConTech Lab – en del af Molio** i forbindelse med analyseprojektet *Sikkert digitalt samarbejde i byggeriet* (august 2025 – januar 2026).

Projektet, som kortlægger byggebranchens digitale sårbarheder og løsninger, der styrker sikkerheden i det digitale samarbejde, er udført i et samarbejde mellem **DI Byggeri, Implement Consulting Group, COWI, Molt Wengel, Molio, BuildingSMART Denmark** og **ConTech Lab**.

Grafisk design og opsætning af Chris Adam for **Crash Creative**.

ConTech Lab er byggebranchens fælles udviklingsplatform, hvor byggeriets virksomheder sammen kan udvikle og eksperimentere med nye måder at benytte data, digitalisering og teknologi på til at skabe fremtidens byggeri – et mere bæredygtigt og produktivt byggeri.

ConTech Lab deler al viden og læring, så det kommer hele branchen til gode.

Indholdsfortegnelse

1.0	Læsevejledning	04
2.0	Introduktion	07
3.0	Del 1: Den digitale trussel i byggebranchen	08
3.1	Byggeriets digitale set-up	10
3.2	Risikobilledet	12
3.3	Sårbarheder på kontoret, på byggepladsen og i skyen	14
3.4	Byggeriets IT-kultur	16
3.5	Byggeriets særlige sårbarheder	19
4.0	Del 2: Løsningskatalog	20
4.1	Risikokortlægning som første skridt	22
4.2	Governance og ansvarsfordeling	24
4.3	Tekniske kontroller	26
4.4	Organisatoriske tiltag	27
4.5	Virksomhedens modenhedsniveau	30
4.6	Data-klassifikation i byggeprojekter	31
4.7	Krav om digital sikkerhed	34
4.8	Standarder der er relevante for det digitale samarbejde	35
4.9	Tilgængelige værktøjer	36
5.0	Håndtering af sikkerhedshændelser og beredskab i byggeprojekter – hvad gør vi hvis det går galt?	38
5.1	Hvad er en sikkerhedshændelse i byggeriet?	40
5.2	Et "light"-beredskab til byggeprojekter	41
6.0	Hvilke løsninger mangler byggebranchen	42
7.0	Tjeklister	46
8.0	Digitale løsninger du skal holde øje med	48
9.0	Afrunding	52
10	Ordliste	55

1.0

Læsevejledning

Publikationen samler viden og indsigter fra dialog med eksperter, workshops med virksomheder i byggebranchen, interviews, spørgeundersøgelse samt desk research.

Publikationen er opdelt i to dele:

Del 1: Den digitale trussel i byggebranchen

Del 1 beskriver trusselsbilledet og byggeriets særlige risikoforhold, herunder branchens digitale set-up, IT-kultur, sammensatte værdikæde samt byggeprojekters faseskift. Formålet er at give et fælles sprog og et risikooverblik, som virksomheder kan bruge som inspiration til egne risikovurderinger.

Del 2: Løsningskatalog

Del 2 præsenterer relevante krav samt anbefalede greb og værktøjer til at styrke sikkert digitalt samarbejde i byggebranchen. Fokus er på risikokortlægning, krav i udbud og kontrakter, fælles projektpraksis (herunder IKT), konkrete tekniske og organisatoriske indsatser samt eksempler på relevante værktøjer og løsninger.

Bagerst i publikationen findes en ordliste med forklaringer og definitioner.

Hvem kan bruge publikationen – og hvordan?

Publikationen kan anvendes af alle aktører i bygge- og anlægsbranchen, men med forskellige formål:

- **Bygherrer og investorer** kan bruge publikationen til at stille klare, risikobaserede krav til digital sikkerhed i udbud, kontrakter og governance.
- **Rådgivere** kan bruge den til at integrere risikovurdering og informationssikkerhed i projektering, modellering og samarbejdsprocesser.
- **Entreprenører** kan bruge den til at etablere sikre samarbejdsplatforme, adgangsstyring, netværkspraksis på byggepladsen samt fælles procedurer med projektets parter.
- **Underentreprenører og leverandører** kan bruge den til at forstå forventninger og minimumniveauer, samt dokumentere egen modenhed og efterlevelse.

Sådan kan publikationen omsættes til handling

Som læser kan du bruge publikationen på tre måder:

- **Som inspiration til kortlægning af eget risikobillede** (virksomhed, leverandørkæde eller konkret byggeprojekt).
- **Som tjekliste ved projektopstart**, fx til krav i udbud, valg af platforme, adgangsstyring og aftaler om ansvar.
- **Som reference for fælles praksis** i igangværende byggeprojekter, hvor sikkerhed skal følges op løbende og dokumenteres.

Afgrænsning og scope

Denne publikation har fokus på sikkert digitalt samarbejde i bygge- og anlægsprojekter. Omdrejningspunktet er de digitale arbejdsgange, systemer og dataudvekslinger, der opstår, når mange virksomheder samarbejder på tværs af byggeriets værdikæde.

Publikationen behandler især:

- Samarbejde på tværs af bygherre, rådgivere, entreprenører, underentreprenører og leverandører.
- Fælles datamiljøer og projektplatforme (CDE, projektweb, cloud-løsninger).
- Adgangs- og rettighedsstyring i projekter med mange aktører og faseskift.
- Netværk og digital infrastruktur på byggepladsen.
- Operationel teknologi (OT), fx maskiner, kraner og sensorer.
- Governance, roller, ansvar, kultur og adfærd i det digitale samarbejde.

Fokus er dermed ikke kun på teknisk it-sikkerhed, men på samspillet mellem teknologi, mennesker og processer i det tværgående samarbejde. Der lægges primær vægt på de tidlige faser og udførelsesfasen i byggeprojekter, hvor rammer for digitalt samarbejde fastlægges, og hvor de største praktiske sårbarheder opstår. Drift og vedligehold berøres i det omfang, beslutninger i projektfasen har betydning for informationssikkerhed og robusthed senere i bygningens livscyklus.

Hvad dækker publikationen ikke?

For at sikre et klart fokus dækker publikationen ikke:

- Detaljerede tekniske konfigurationer eller produktanbefalinger.
- Konkrete beskrivelser af sårbarheder på specifikke byggepladser eller i navngivne projekter.
- Dybdegående behandling af cybersikkerhed i driftsfasen af bygninger (facility management, smart buildings mv.), medmindre det har direkte relevans for selve byggeprojektets digitale samarbejde.
- Juridisk rådgivning i snæver forstand (publikationen beskriver rammer og opmærksomhedspunkter, men erstatter ikke konkret juridisk eller teknisk rådgivning).

.....



 DI Byggeri

.the tech collective
powered by Implement

COWI

MOLT | WENGEL

MOLIO
viden, du bygger på

 buildingSMART®
Danmark

CON
TECH
LAB_

Introduktion

Digitalt samarbejde er blevet en forudsætning for effektivt byggeri, men det har også gjort branchen mere sårbar. Bygge- og anlægsprojekter involverer mange aktører, skiftende faser og omfattende datadeling på tværs af virksomheder og platforme. Det betyder, at en sårbarhed ét sted i værdikæden kan få konsekvenser mange andre steder. Derfor kræver cybersikkerhed i byggeriet ikke kun fokus på den enkelte virksomhed, men også fælles metoder, klare krav og en praksis, der fungerer i hverdagen ude på byggepladsen.

De fem vigtigste pointer du skal tage med dig er:

- **Værdikæden er angrebsfladen.** Cyberangreb rammer ofte gennem det svageste led. Sikkerhed skal derfor tænkes på tværs af virksomheder, leverandører og samarbejdsplatforme på byggeprojekter.
- **Projektplatforme og adgangsstyring er nogle af de største praktiske risikopunkter.** Uklare roller, brede adgange og manglende nedlukning af adgange skaber unødvendig risiko, særligt når projekter skifter faser og deltagere.
- **Byggepladsens netværk og OT udgør en voksende sårbarhed.** Ét fælles netværk til alt, manglende segmentering og udstyr uden opdateringer giver nye indgange, og kan i værste fald få sikkerhedsmæssige, økonomiske og driftsmæssige konsekvenser.

Denne publikation er udarbejdet som del af analyseprojektet *Sikkert digitalt samarbejde i byggeriet* (august 2025 – januar 2026). Den beskriver byggeriets særlige risikobillede og peger på løsninger, der kan styrke sikkerhed og robusthed i digitale samarbejder, uden at hæmme fremdrift og produktivitet.

- **Kultur og adfærd er ofte den afgørende faktor.** Awareness, træning og fælles vaner er blandt de mest omkostningseffektive indsatser, og er nødvendige for at sikre efterlevelse i praksis.
- **Sikkerhed skal tænkes ind fra start, og følges op på løbende.** Risikokortlægning, klare krav i udbud/kontrakter, IKT-aftaler og kontinuerlig opfølgning gør sikkerheden styrbar og dokumenterbar gennem hele projektets livscyklus.

Bag projektet *Sikkert digitalt samarbejde i byggeriet* er **DI Byggeri, Implement Consulting Group, COWI, Molt Wengel, Molio, BuildingSMART Denmark** og **ConTech Lab**.

3.0 Del 1

Den digitale trussel i byggebranchen

Byggeriets virksomheder er, ligesom alle andre danske virksomheder, under et konstant risikotryk. Styrelsen for Samfundssikkerheds "Trusselsvurdering af Cybertruslen mod Danmark 2025" fastslår, at cybertruslen er blevet et grundvilkår. Myndigheder, virksomheder og borgere udsættes dagligt for angreb fra både statslige og ikke-statslige aktører¹.

Phishing er fortsat den mest udbredte angrebstype². Angrebene er ofte ikke målrettet én virksomhed, men gennemføres på baggrund af store mængder e-mailadresser, som handles ulovligt.

Samtidig vinder "social engineering" frem som metode. Her manipulerer gerningspersonen mennesker til at afsløre følsomme oplysninger eller udføre handlinger, der kompromitterer sikkerheden, ofte ved at udgive sig for en troværdig afsender og bruge efterligning, pres eller overtalelse³.

For bygge- og anlægsbranchen kan angreb også ske på og med operationel teknologi (OT), fx maskiner, kraner, ventilation og sensorer. Når OT kobles på netværk, opstår nye angrebsflader. I værste fald kan materiel påvirkes eller fjernstyres, eller sikkerhedssystemer kompromitteres.

I følge PWC's Cybercrime Survey 2025⁴, angiver 32% af virksomhederne, at de har været udsat for en sikkerhedshændelse. Blandt de ramte virksomheder er phishing den mest udbredte hændelsestype (62%). Derudover rapporteres DoS-angreb (28%), leverandørfejl (25%) og utilsigtet deling af følsomme oplysninger (23%) som hyppige hændelser.

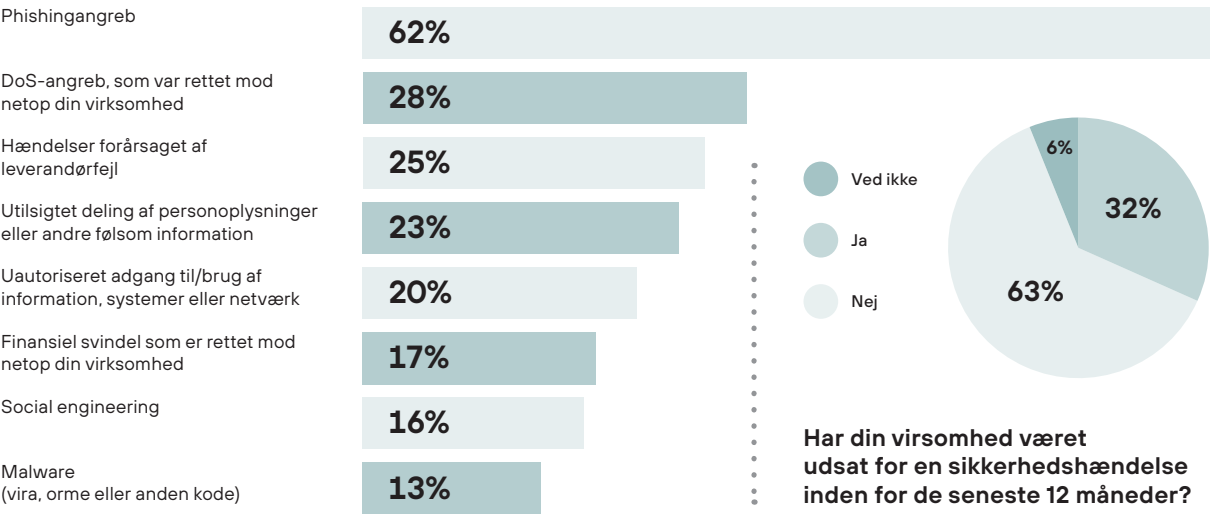
¹ samsik.dk/publikationer/cybertruslen/

² PWC's Cybercrime Survey 2025

³ Cybersikkerhed: social engineering - Consilium

⁴ PWC's Cybercrime Survey 2025

Hvilken type sikkerhedshændelse(r) er der tale om?



Eksempel: Bouygues, Frankrig

Bouygues, et stort franskejdet entreprenørselskab, blev i 2020 ramt af et ransomware-angreb, som begyndte med phishing e-mails. Med et "fladt netværk", hvor systemer hænger tæt sammen uden segmentering, kunne angriberne bevæge sig hurtigt og frit rundt, når de først var inde i systemet. Konsekvensen var nedlukning af mange byggepladser i tre uger og et anslået økonomisk tab på 7,5 mia. DKK.

Eksemplet viser, hvordan ét klik på et falsk link, kan få uforholdsmæssigt store konsekvenser for rigtig mange aktører på tværs af et byggeprojekts værdikæde.

3.1

Byggeriets digitale set-up

En væsentlig del af byggeriets risikobillede er relateret til branchens lange værdikæde:

En virksomhed kan blive ramt, fordi angriberen finder et svagt led hos en samarbejdspartner eller leverandør.

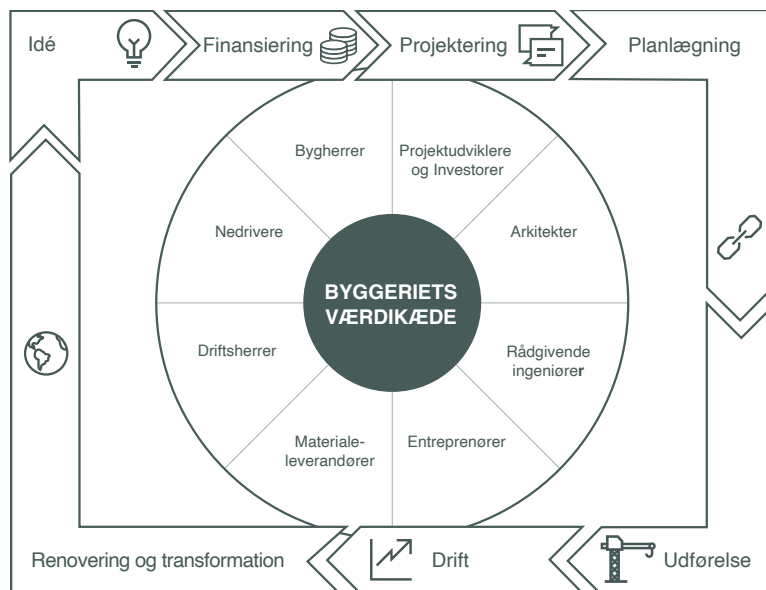
■ ■ Byggeriet er en branche, der netop er præget af mange led, og virksomheder indgår i utallige partnerskaber og samarbejder på tværs af værdikæden – især digitalt. Derfor skal cybersikkerhed inden for byggeriet tænkes meget bredere end bare virksomhedens egne it-systemer.

Malene Stidsen
Programchef for cybersikkerhed i Industriens Fond

Derfor er det afgørende at tænke i værdikædesikkerhed:

- Hvem har adgang til data?
- Hvem kan påvirke systemer?
- Hvilke platforme binder samarbejdet sammen?

Bygge- og anlægsprojekter strækker sig ofte over flere år og gennemgår flere faser, hvor både governance og projektledelse kan ændre karakter. Det betyder, at it-governance og sikkerhedsprocedurer kan blive utydelige eller inkonsistente.



Faseskift, som fx fra planlægning til udførelsen, kan gøre det vanskeligt at fastholde ansvar for blandt andet platforme, adgangsstyring, datadeling og beredskab. Og projektets praksis kan i perioder komme i konflikt med virksomhedernes egne politikker om fx fildeling og sikkerhed.



3.2 Risikobilledet

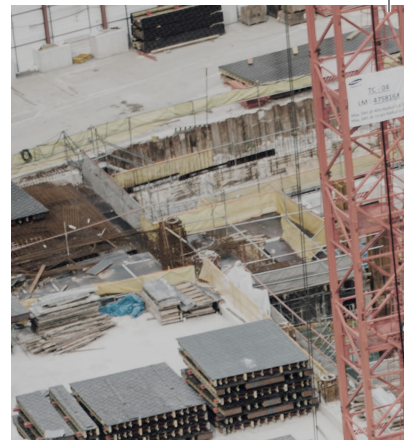
I Nationalt Risikobillede 2025⁵ opfordrer Styrelsen for Samfundssikkerhed virksomheder til at udarbejde deres eget risikobillede. Som støtte til byggebranchen har projektpartnerne bag projektet "Sikkert digitalt samarbejde", og med input fra branchen, udarbejdet et samlet risikobillede for byggeriet, som kan bruges som inspiration til virksomheders egne risikovurderinger samt vurdering af risici i leverandørkæder og samarbejder.

Byggeriets risikobillede peger på følgende centrale forhold:

IT-kultur og sikkerhedsvaner

Mange virksomheder mangler klare politikker for it-sikkerhed, og medarbejderne er ikke uddannet i sikker brug af systemerne.

⁵ Nationalt Risikobillede 2025 – Danmarks væsentligste risici og trusler



Sammenkædede systemer

Mange systemer, platforme og processer er gensidigt afhængige i et byggeprojekt. Nedbrud ét sted kan skabe dominoeffekt, også i betalinger og leverancer, hvis en central aktør eller leverandør rammes.

Manglende opdateringer og legacy-systemer

Forældede systemer uden opdateringer udgør en særlig risiko, især hvis de er koblet til moderne platforme.

Simple digitale netværk på byggepladsen

Mange byggepladser har simple/flade netværk, hvor segmentering og dobbeltbeskyttelse mangler. Når "alt hænger sammen", kan en angriber bevæge sig frit rundt mellem systemer og data efter første adgang.

Mangelfuld bruger- og rettighedsstyring

Adgange gives ofte bredt af hensyn til fremdrift. Det kan betyde, at underentreprenører og andre får adgang til fortrolige oplysninger, de ikke har behov for, og at adgange ikke fjernes, når de ikke længere er relevante.

OT – operationel teknologi

Maskiner, kraner, ventilation og sensorer kobles på netværk, og softwareopdateringer sker ikke automatisk. Digitalisering af OT giver nye muligheder, men også nye sårbarheder. I værste fald, kan nogen fjernstyre en kran eller pille ved sikkerhedssystemer.

Mange samarbejdspartnere og faseskift

Byggeprojekter involverer mange forskellige og skiftende aktører (entreprenører, underentreprenører, materialeleverandører, m.fl.) som ofte har forskellig modenhed med hensyn til cybersikkerhed. Det øger risikoen for svage led og uklare ansvarsplaceringer.

Fysisk adgang til byggeriet

Byggepladser har mange besøgende og midlertidige medarbejdere. Det gør det vanskeligt at have fuldt overblik over, hvem der har adgang til hvad både fysisk og digitalt.

3.3

Sårbarheder på kontoret, på byggepladsen og i skyen

Digitalisering har udvisket grænsen mellem kontor og byggeplads. Teknologien forbinder alt, og derfor hænger cybersikkerheden i de to miljøer tæt sammen.

På kontoret ligger mange løsninger i skyen. Sårbarheder kan derfor være skjulte, fx når data flyttes mellem regioner, eller når netværks- og sikkerheds-konfigurationer ikke vedligeholdes systematisk.

En særlig kritisk sårbarhed er projektplatforme til dokument-, informations- og datadeling. Platformene finansieres ofte af bygherre, men administreres af rådgiver eller entreprenør.

I praksis er rettighedsstyring ikke altid konsekvent: deltagere kan få adgang til mere end nødvendigt, og adgange lukkes ikke altid ned efter endt behov.

Entreprenørens digitale landskab

Projekter og produktion				Økonomi og support	Tilbud og kalkulation	IT og support
Webapp med skemaer	CDE - projektvalg	Officepakke	Fakturaflow Continia	ERP Nav	SIGMA	Filserver
Sagsdrev	Excel-ark	Bluebeam	Timer, udlæg, km Expandit	Rapporter YellowFinn	GYB markeds-analyse	PC
Sagsmail	Print	MSP		EAN Spoon Connect	Adobe Design	Mobil
DWG viewer	TactPlan/ MSP	Solibri		Løn Lessor	A&K skemaer	Internet
Special apps fx Danalock	Frame DGNB	MS Teams				Software portal
						IT support

Kilde HD Lab, eksempler på digitale værktøjer i byggeriet

Uhensigtsmæssig brug af digitale værktøjer øger også risikoen. Excel bruges fx mange steder til at styre kritiske funktioner som budgetter, tidsplaner, kontrakter og ressourcer, hvor der i stedet burde anvendes sikre systemer. Gamle regneark sendes rundt, versionsstyring er begrænset, og sikkerheden er ofte utilstrækkelig. Det kan skabe både sikkerhedsrisici og fejl i kritiske beslutningsgrundlag.

På byggepladsen opstår sårbarheder især ved brug af ét fælles Wi-Fi til både droner, tablets, kameraer, sensorer og private enheder. Samtidig er der mange personer med varierende tilknytning til pladsen, fra faste virksomhedspartnere, der indgår som en del af byggeprojektet, til materialeleverandører der måske kun kommer på byggepladsen en enkelt gang eller to. Det øger risikoen for uautoriseret adgang og manglende efterlevelse af procedurer.

Endeligt skaber brugen af private enheder (BYOD) til arbejdsopgaver yderligere indgange, som virksomheden ikke har fuld kontrol over i deres it-infrastruktur. Bliver en medarbejders device hacket privat, kan angriberen måske få adgang til virksomhedens software, og omvendt.

3.4

Byggeriets IT-kultur

Byggeriets indsatser for IT-sikkerhed vurderes generelt at være mangelfulde sammenlignet med andre brancher.

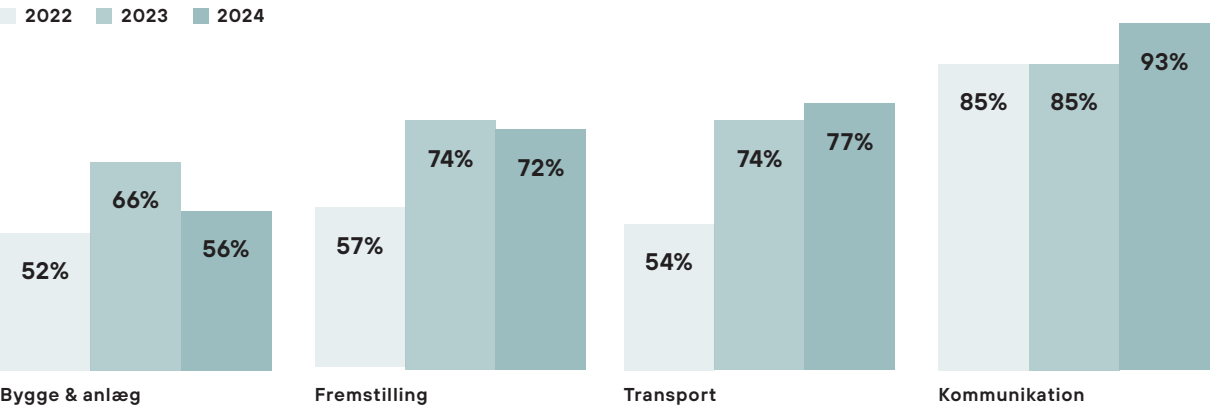
Danmarks Statistiks undersøgelse i foråret 2024⁶ om IT-anvendelse i små virksomheder viser, at små virksomheder indenfor byggeri og anlæg typisk har mest fokus på softwareopdateringer (79%), backup til alternativ placering (76%) og adgangskontrol til netværk (59%). Men på 13 ud af 15 foranstaltninger man kan tage som virksomhed ligger branchen under de øvrige brancher (industri, handel/transport, information/kommunikation og erhvervsservice).

Kompetenceudvikling er en særlig svaghed. Kun 24% af virksomhederne i byggeriet tilbyder frivillig uddannelse/træning, og kun 16% har obligatorisk uddannelse. 26% har information om it-sikkerhed via skriftlig kontrakt, og 22% har gennemført en risikoanalyse.

Industriens Fonds Cyberbarometer 2024⁷, viser desuden, at hvor de fleste brancher har øget antallet af cybersikkerhedstiltag over tid, gælder det i mindre grad for byggeri og anlæg.

Branchen har både færrest tiltag og den mindste stigning.

Figuren viser udviklingen i det gennemsnitlige antal cybersikkerheds tiltag på tværs af brancher fra 2022 til 2024⁸.



⁶ NYT: Øget it-sikkerhed i små virksomheder - Danmarks Statistik

⁷ Cyberbarometer 2024 | Cybersikkerhed

⁸ Cybersikkerhed & konkurrencefordele blandt danske SMV'er 2024

Sikkert digitalt samarbejde i byggeriet:
Spørgeskemaundersøgelse

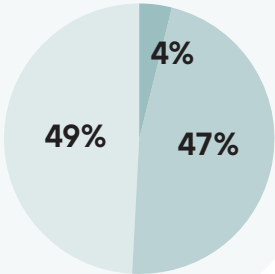
I projektet er der gennemført en spørgeskemaundersøgelse blandt byggeriets virksomheder, om hvordan de arbejder med sikkert digitalt samarbejde.

Resultaterne viser, at det kun er omkring en fjerdedel af virksomhederne, der har et fælles aftalt minimumniveau for cybersikkerhed på et projekt eller byggeplads, og kun knap halvdelen anvender sikre krypterede systemer til at dele data.

Blandt de hyppigst nævnte sårbarheder er deling af Excel-ark og links til projektmapper.

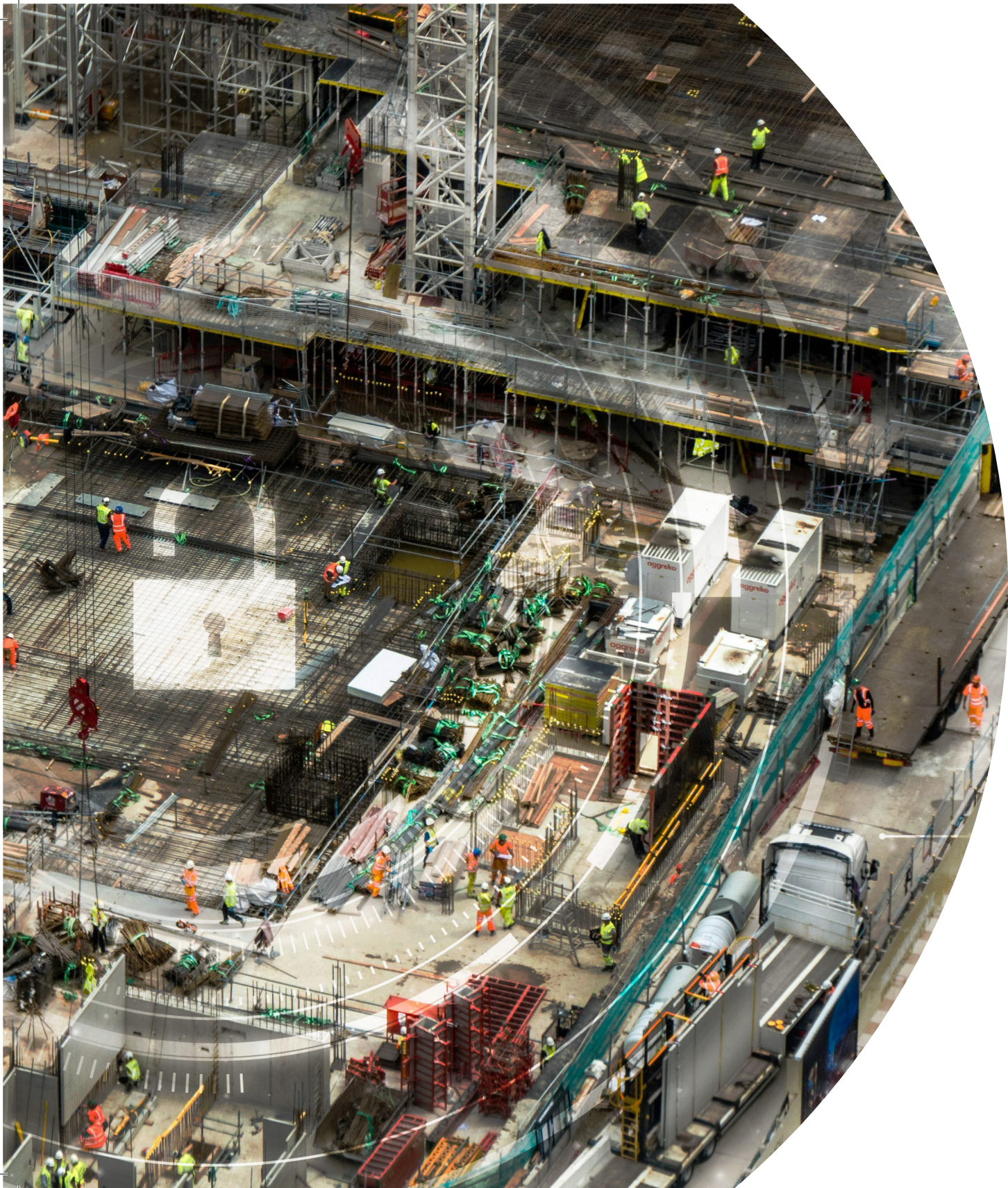
Hvordan deles projektdata mellem parterne?

- Uden særlige sikkerhedsforanstaltninger
- Typisk via almindelig mail eller fildeling med visse forholdsregler
- Gennem sikre, krypterede kanaler eller godkendte systemer



IT-sikkerhedsforanstaltninger i små virksomheder fordelt på brancher i 2024

Figuren viser resultaterne fra Danmarks Statistiks spørgeskema	Alle	Industri	Bygge og anlæg	Handel og transport	Information og Kommunikation	Erhvervs service
	Pct. af alle små virksomheder					
Mindst én type foranstaltning	92	97	91	90	98	94
Stærke adgangskoder	55	51	45	55	75	59
Systematisk opdatering af software	82	84	79	79	88	86
Biometriske metoder til brugerid.	23	18	24	19	41	28
Mindst to godkendelsesmekanismer	47	48	38	41	80	54
Kryptering af data, filer eller e-mails	39	36	27	33	68	54
Backup til en alternativ placering	80	86	76	75	93	86
Adgangskontrol til netværk	69	73	59	67	85	75
VPN (virtuelt privat netværk)	41	38	31	38	56	53
It-sikkerhedsovervågningssystem	51	48	40	50	74	60
Lagring af logfiler	48	44	28	48	73	62
Risikoanalyse	36	30	22	35	66	48
Tests af it-sikkerhed	34	28	23	33	57	42
Dokumentation om it-sikkerhed	45	41	29	41	75	59
Mindst én type info om it-sikkerhed	59	57	46	56	88	71
Frivillig uddannelse og træning	43	36	24	42	73	57
Obligatorisk uddannelse og træning	29	24	16	27	58	40
Via skriftlig kontrakt	34	31	26	29	64	44



3.5

Byggeriets særlige sårbarheder

Som beskrevet skaber byggeriets særlige forhold, IT-kultur og begrænsede sikkerhedsindsatser et sæt gennemgående sårbarheder. Listen her er ikke udtømmende, men fremhæver de mest centrale sårbarheder identificeret i projektet:

.....

- Udbredt brug af simple passwords og genbrug på tværs af projekter og portaler, ofte uden password manager og multifaktorgodkendelse.
- Deling af links til projektmapper, hvor adgange ikke begrænses til "need-to-know", og hvor adgang ofte består længe efter endt behov (manglende rettighedsstyring og nedlukning).
- Serveres fysiske placering og mangelfuld sikring kan udgøre en sårbarhed.
- Bildata kan give adgang til mobilitets-infrastruktur gennem biler, der står på byggepladsen.
- USB-stik anvendes til deling af data og dokumenter, og kan overføre malware uden at blive opdaget.
- Offentlige udbud med komplet beskrivelse af projektet giver uønsket indsigt i kritiske forhold, hvis materiale er frit tilgængeligt på kommunernes hjemmeside.
- Manglende uddannelse i it-sikkerhed øger risikoen for phishing og social engineering.
- Midlertidige medarbejdere og gæster på byggepladsen kender ofte ikke sikkerhedsprocedurer.
- Fælles Wi-Fi til "alt" uden segmentering, og i nogle tilfælde uden tilstrækkelig adgangskontrol.
- Deling af dokumenter via usikre platforme, e-mail eller åbne cloud-links (fx Dropbox/WeTransfer).
- Backup er ikke altid automatiseret, og restore testes ikke systematisk, hvilket forværrer konsekvenser ved ransomware.
- Tablets og smartphones bruges til kritiske opgaver uden MDM (Mobile Device Management).
- Ældre systemer kører uden opdateringer og udgør kendte sårbarheder.

4.0

Del 2

Løsningskatalog

Digitalt samarbejde gør byggeprojekter mere effektive, men betyder også, at projektets aktører skal arbejde mere struktureret med digital sikkerhed. Et læk af konstruktionstegninger, tidsplaner eller driftsdata kan få konsekvenser for både mennesker, forretning og omdømme. Derfor bør informationssikkerhed ses som en integreret del af professionel projektledelse.

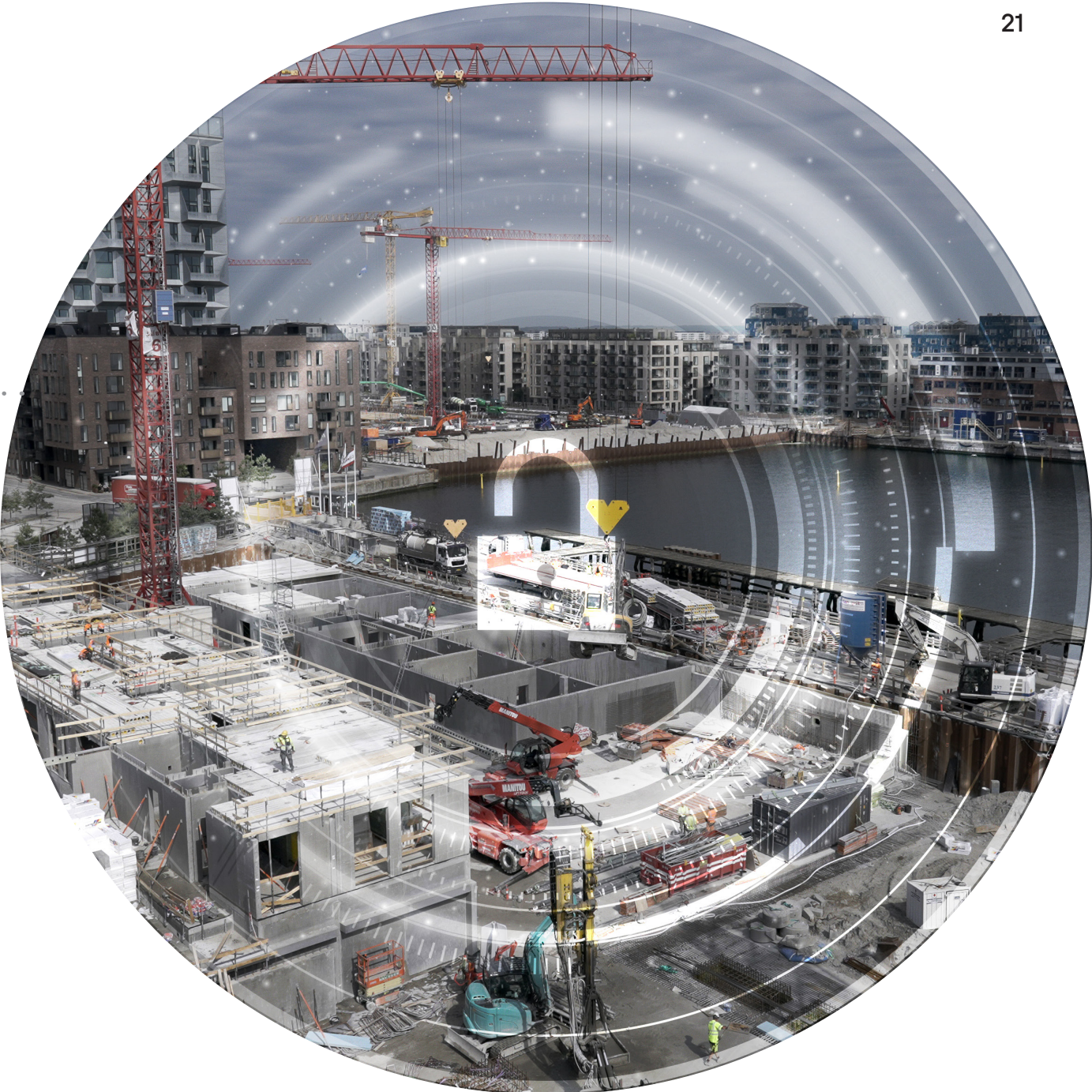
Sikkert digitalt samarbejde handler om at understøtte samarbejdet, reducere fejl og skabe tryghed for alle involverede i et byggeprojekt. God IT-styring og datakvalitet reducerer risiko, øger fremdriften og gør det nemmere at dokumentere efterlevelse af krav.

Cybersikkerhed er dermed ikke længere et isoleret IT-anliggende, men et konkurrenceparameter og en forudsætning for robusthed i fremtidens byggeri. Det kræver, at virksomheder ikke kun har styr på egen sikkerhed, men også på sikkerheden i leverandørkæden og i samarbejdsrelationer. Branchen har behov for et kulturskifte, hvor digital sikkerhed bliver en naturlig del af udbud, samarbejde og projektstyring – understøttet af fælles metoder og værktøjer.

■ *Digitaliseringen gør byggebranchen mere effektiv, men også mere sårbar. Når byggepladsen er lige så digital som fysisk, bliver cybersikkerhed et driftsspørgsmål, som vi skal behandle på linje med arbejdsmiljø og kvalitetssikring. Grundlæggende styrker vi produktiviteten, tilliden og robustheden i vores projekter, når vi sammen med branchen tager ansvar for sikkerheden i vores digitale samarbejde.*

Søren Cajus
Chef for byggeri og teknologi hos DI Byggeri

Formålet med løsningskataloget er at beskrive fælles krav, metoder og digitale løsninger, som branchen kan tage udgangspunkt i for at øge sikkerheden og samtidig understøtte effektiv projektgennemførelse.



4.1

Risikokortlægning som første skridt

En grundlæggende forudsætning for bedre digital sikkerhed på bygge- og anlægsprojekter er en systematisk risikokortlægning eller analyse. I dag er det kun knap en femtedel af alle projekter og byggepladser, der fast gennemfører en sådan kortlægning⁹.

Er der gennemført risikovurdering ift. cybersikkerhed i projekter og på byggepladser?

Ja, det er et fast punkt i vores projektgrundlag og planer for byggepladsen

17%

Kun i enkelte projekter/byggepladser

37%

Nej, det er ikke gennemført

46%

Kortlægningen fokuserer på trusler, sårbarheder, konsekvenser og sandsynlighed. Baseret på kortlægningen kan man lave en risikovurdering baseret på sandsynlighed × konsekvens, som gør det muligt at prioritere indsatsen, så den står mål med risikoen.

Efter risikovurderingen formuleres indsatser til risikobehandling.

Det kan være:

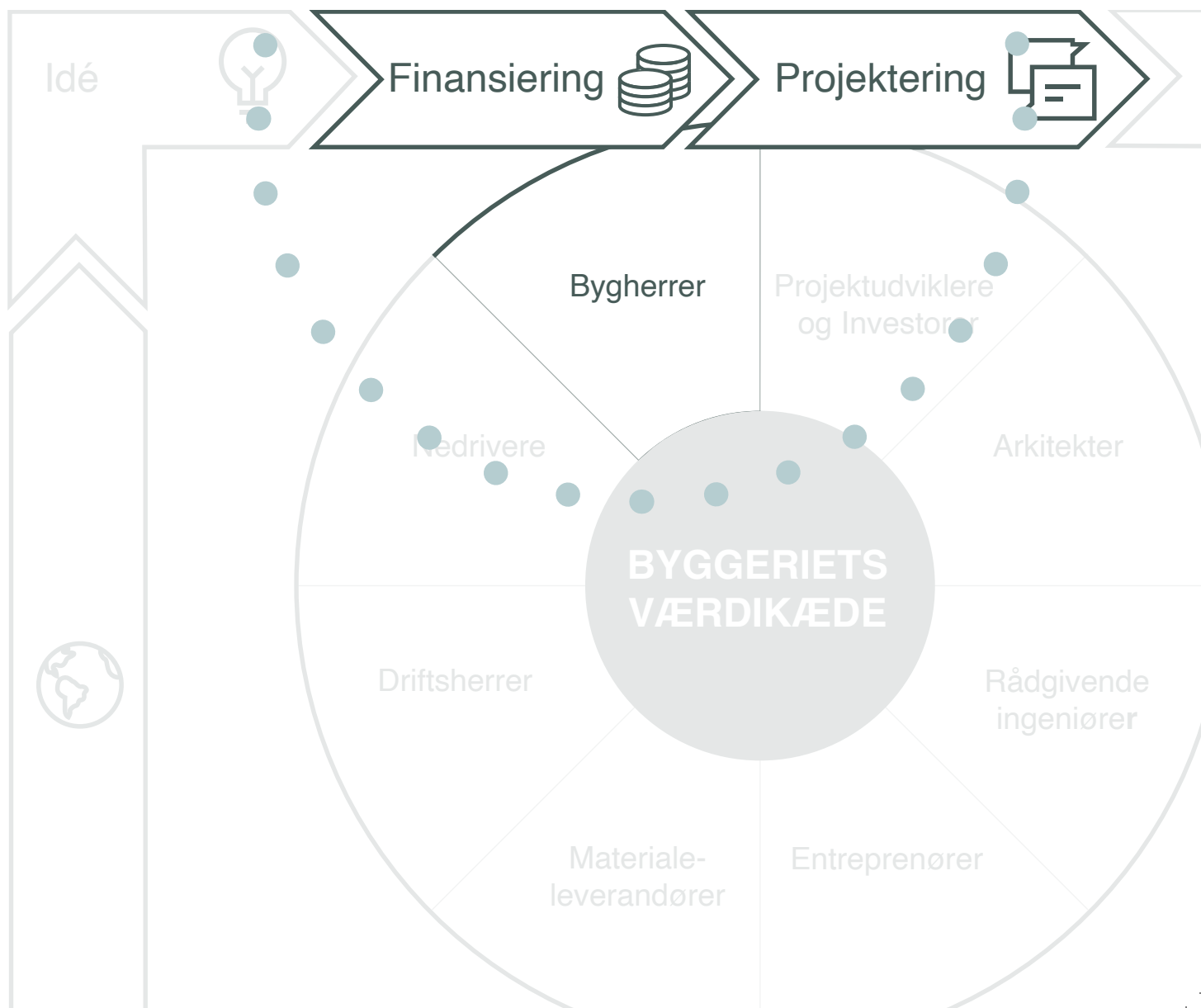
- **Governance**
(roller, ansvar, processer)
- **Tekniske kontroller**
(adgangsstyring, kryptering, backup)
- **Organisatoriske tiltag**
(awareness, træning, kvalitetssikring)

Risikokortlægning bør gennemføres tidligt i byggeprocessen, allerede inden projekteringsfasen, og løbende revurderes, også når byggepladsen etableres og er aktiv. Kortlægningen bør beskrive, hvilke data og informationsaktiver der indgår, hvor kritiske de er, og om projektet samlet set kan være omfattet af regulatoriske krav.

■ *Fremtidens byggeprojekter, særligt dem der berører kritisk infrastruktur, kræver en risikobaseret tilgang til digital sikkerhed. Det handler om at forstå, hvor projektets reelle sårbarheder ligger, og bygge governance, processer og samarbejdsmodeller op omkring dem. Først dér skaber vi reel resiliens.*

Emil Sahin
Associate Technical Director i COWI

⁹ ConTech Lab Cyber Survey 2026



4.2

Governance og ansvarsfordeling

Klarhed om ansvar er en forudsætning for sikkert digitalt samarbejde.

En stor del af byggeriets digitale samarbejde foregår i dag i skybaserede løsninger og fælles projektplatforme. Her opstår ofte en grundlæggende misforståelse: at sikkerheden "ligger hos leverandøren".

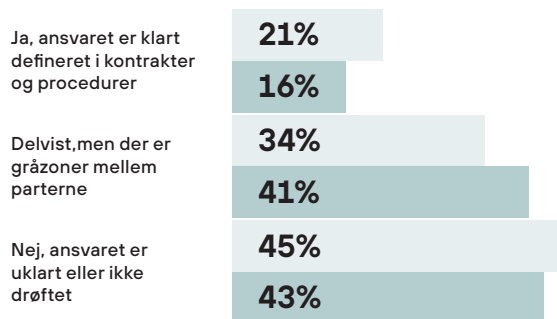
I praksis er ansvaret for at håndhæve de forskellige opgaver relateret til cybersikkerhed delt, og hvis det ikke er tydeligt aftalt, opstår der huller i sikkerheden.

I byggeprojekter, hvor platforme ofte betales af bygherre, administreres af rådgiver eller entreprenør og anvendes af mange parter, er risikoen for uklarhed særligt stor.

Manglende afklaring kan føre til for brede adgange, manglende nedlukning af brugere, uklare beredskabsprocedurer og i sidste ende øget risiko for databrud.

Er det tydeligt, hvem der har ansvaret for datasikkerhed i de forskellige faser af jeres projekter? (f.eks projektering, tilbudsgivning, udførelse)

Er det tydeligt, hvem der har ansvaret for datasikkerhed på de forskellige områder af jeres projekter? (et område kan f.eks være IoT)



Ansvaret for de delte opgaver betyder, at sikkerheden er fordelt mellem flere parter, og at hver part har ansvar for forskellige dele af den samlede sikkerhed.

En forenklet model for delte opgaver i byggeprojekter kan beskrives således:

Platform- og cloudleverandøren:

- Drift og teknisk stabilitet af platformen.
- Grundlæggende teknisk sikkerhed (fx datacentre, netværk, fysisk sikring).
- Indbygget sikkerhed i platformen (fx kryptering, backup-muligheder, logging).

Bygherren:

- Overordnede krav til informationssikkerhed i projektet.
- Fastlæggelse af risikoniveau og dataklassifikation.
- Krav til brug af platforme i udbud og kontrakter baseret på NIS2, CER og ISO 19650 (jf. afsnit 4.7 og 4.8 for mere information om krav og standarder).

Rådgiveren/entreprenøren:

- Integrere risikovurderinger i projektering og modellering.
- Daglig administration af projektplatformen.
- Oprettelse, ændring og lukning af brugere og rettigheder.
- Sikring af korrekt brug af platformen i projektets faser.

Den enkelte projektdeltager:

- Korrekt brug af systemer og platforme.
- Beskyttelse af egne login-oplysninger.
- Overholdelse af aftalte procedurer for deling og opbevaring af data.
- Dokumentere deres egen sikkerhedsmodenhed ift. krav fra hovedaktører.

Hvis én af disse roller ikke er tydeligt defineret, opstår der et sikkerhedsmæssigt "tomrum".

Typiske faldgruber i byggeprojekter:

Erfaringer fra projektet peger på en række tilbagevendende udfordringer:

- Ingen har det klare ansvar for at lukke adgange ved faseskift eller projektets afslutning.
- Platformens sikkerhedsfunktioner (fx logning, MFA, rettighedsgrupper) er ikke aktiveret.
- Brugere deler links eller eksporterer data uden for sikre platforme.
- Beredskab ved sikkerhedshændelser er uklart: Hvem gør hvad – og hvornår?

Disse faldgruber skyldes sjældent manglende vilje, men manglende fælles afklaring.

Sådan tydeliggøres ansvar i praksis:

For at omsætte ansvaret for de delte opgaver til praksis bør ansvarsfordelingen:

- Beskrives eksplicit i IKT-aftaler, kontrakter eller projektets governance-dokumenter.
- Knyttes til konkrete roller (ikke kun virksomheder).
- Følges op ved projektopstart og løbende, særligt ved faseskift.

Det anbefales, at der i hvert projekt udpeges en klar ansvarlig for platformadministration og digital sikkerhed, fx en IKT-koordinator eller digital projektleder med mandat til at håndhæve fælles praksis.

4.3

Tekniske kontroller

Tekniske kontroller, der understøtter sikkert digitalt samarbejde dækker blandt andet:

- **Optimering af software**
Software skal vedligeholdes sikkerhedsmæssigt og begrænses eller isoleres mest muligt. Processen med sikkerhedsoptimering af eksisterende software kaldes "hardening", og handler om at fjerne unødige funktioner, lukke sårbarheder og aktivere relevante sikkerhedsindstillinger, som ofte findes i systemerne, men ikke altid udnyttes.
- **Adgangsstyring af netværk**
En anden løsning til styrkelse af den digitale sikkerhed er at have forskellige adgange til forskellige projektpartnere alt efter tilknytning, fx som på hospitaler og skoler: et gæstenetværk, et administrativt netværk og et teknisk/OT-netværk. Det er også afgørende at styrke bruger- og rettighedsstyring, især på projektplatforme, hvor følsom information deles.
- **Scanningsværktøjer**
Sårbarhedsscanning kan give et hurtigt overblik over eksponerede systemer og virksomhedernes digitale berøringspunkter med internettet. Online tjenester som Shodan og Censys kortlægger løbende synlige systemer. Det betyder, at hvis din virksomhed har åbne porte eller eksponerede systemer, er de allerede registreret. Disse oplysninger kan nemt findes af både forskere, konkurrenter, kriminelle og statslige aktører¹⁰.

¹⁰ Du bliver allerede scannet- Spørgsmålet er, om du opdager det (DI Digital)

4.4

Organisatoriske tiltag

Det er vigtigt at opbygge en sikkerhedskultur, der kan fungere på tværs af værdikæden, faseskift og fagligheder.

Awareness og fælles vaner er ofte den mest omkostningseffektive måde at reducere cyberrisici på og samtidig styrke tillid og samarbejde.

Løbende opfølgning og dokumentation af indsatsen hjælper med at fastholde et passende sikkerhedsniveau og skabe læring, der kan forbedre praksis i kommende faser og projekter.

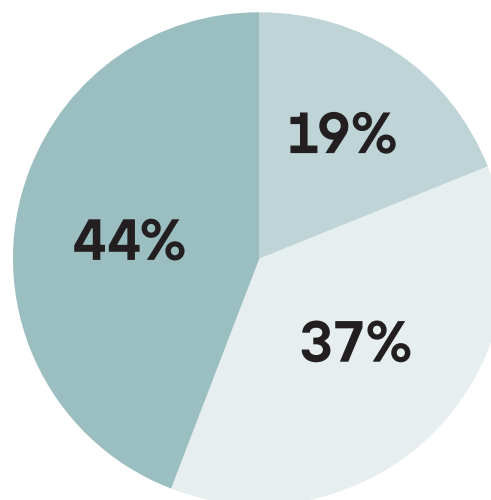
Effektiv awareness-træning

Den største udfordring i arbejdet med cybersikkerhed er som oftest adfærd og det at skabe forståelse, motivation og ansvar hos alle, der arbejder på projektet eller byggepladsen.

Det handler både om sund fornuft, basale sikkerhedsvaner (fx ikke at dele følsomme tegninger via e-mail) og om at reducere menneskelige fejl i en hverdag med højt tempo og mange aktører.

I dag udfører næsten halvdelen af byggeriets virksomheder ikke træning i cybersikkerhed¹¹.

-  **Nej, vi gennemfører ingen træning**
-  **Ja, det gør vi i forbindelse med nyansættelser**
-  **Ja, medarbejderne bliver løbende testet og trænet i cybersikkerhed**



¹¹ ConTech Lab Cyber Survey 2026

Træning virker bedst, når den er kort, relevant og hyppig

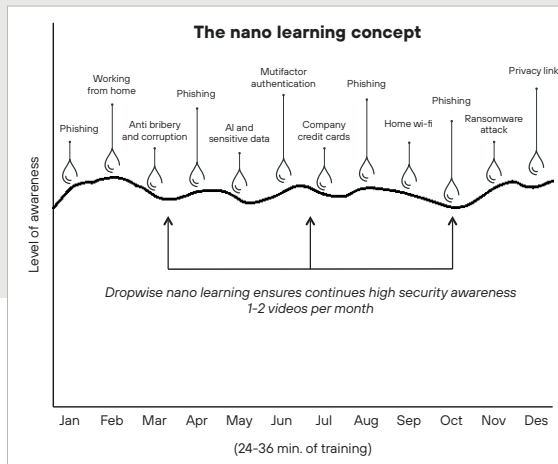
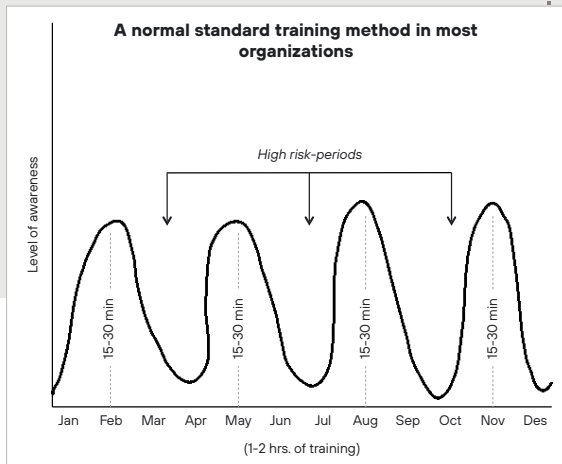
Lange årlige sessioner har begrænset effekt. En effektiv tilgang kan være mikrotæning i moduler på 90–120 sekunder, der udsendes løbende og knytter sig til konkrete, relaterbare risici (fx phishing, deling af links, håndtering af følsomme oplysninger).

Et centralt element er måling og dokumentation. Med de rette systemer kan man følge, hvem der har gennemført træning, hvor risiciene ligger, og hvilke

afdelinger der har behov for en målrettet indsats. På den måde bliver cybersikkerhed både målbar og styrbar.

Der findes også løsninger, hvor medarbejdere skal bestå korte tests for at få adgang til systemer eller arbejdspladser, og de løsninger kan også bruges til byggeprojekter.

Maximize the outcome of the training



- ■ Vi skal engagere folk dér, hvor risikoen er, og integrere krav om awareness-træning i udbuds- og samarbejdsprocesser, så alle parter arbejder efter samme baseline og dokumentation.

Anders Balslev
Partner hos Implement Consulting Group

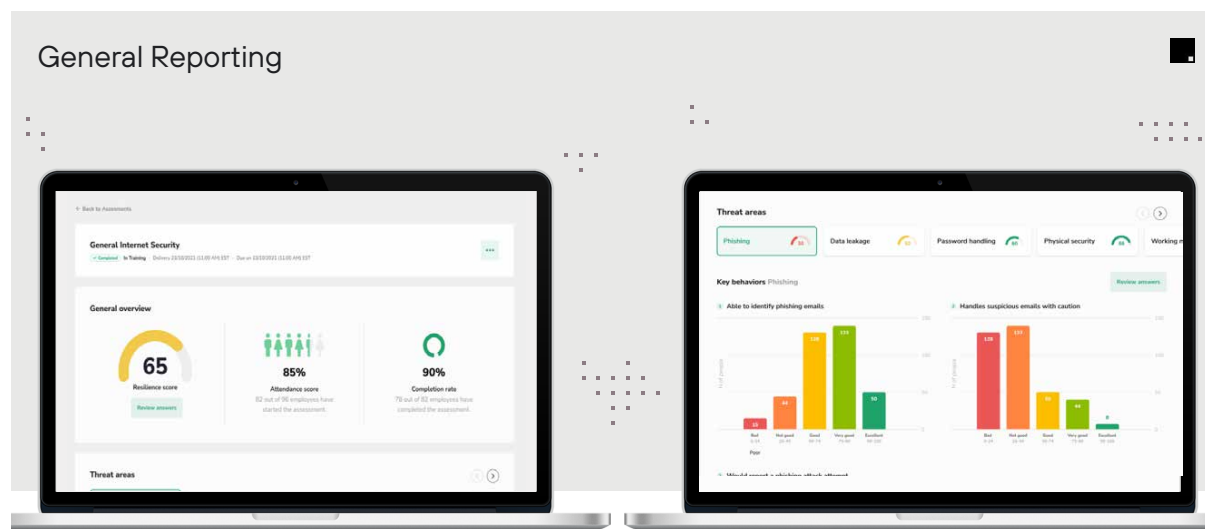
Dog skal man være opmærksom på krav til gennemsigtighed og ligebehandling, særligt i offentlige udbud.

Opfølgning og dokumentation

Det er vigtigt med løbende opfølgning for at sikre, at krav og praksis følges ad. Det kan ske ved at genbesøge risikovurderingen, hvor nye sårbarheder eller indsatser kan blive relevante.

Dokumentation kan forankres i aftaler (fx IKT-aftaler) og i digitale systemer, der registrerer træning og indsatser digitalt.

Som del af et samarbejde kan parter stille krav om kontroller, dokumentationsgennemgang og stikprøver. Dokumentation kan også understøttes af eksterne ordninger som revisorerklæringer, D-mærket eller tilsvarende. (jf. afsnit 4.9 for yderligere information).



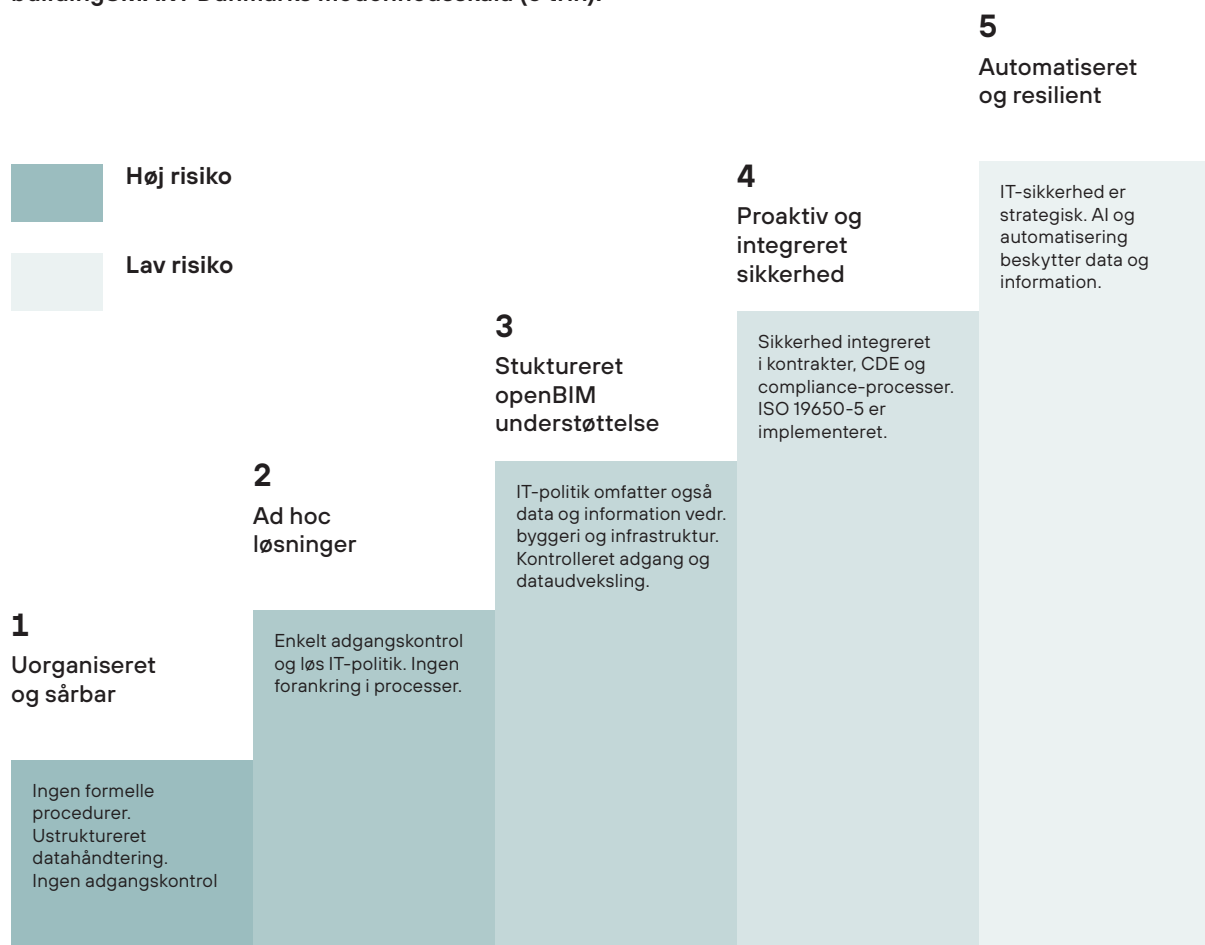
Dashboards allows easy visibility and actions to ensure overview and outlines the progress an organization reaches. All results can be extracted via PDF, open API, integrations and CSV. files to support data workflows for optimal output. Certificate for employees are issued upon completion.

Interactive and real-life situations based on a No blame – No shame methodology

4.5

Virksomhedens modenhedsniveau

Det er en fordel at kende eget modenhedsniveau for at prioritere næste skridt. For byggeprojekter kan der fx tages udgangspunkt i Molt Wengel og buildingSMART Danmarks modenhedsskala (5 trin).



4.6

Data-klassifikation i byggeprojekter

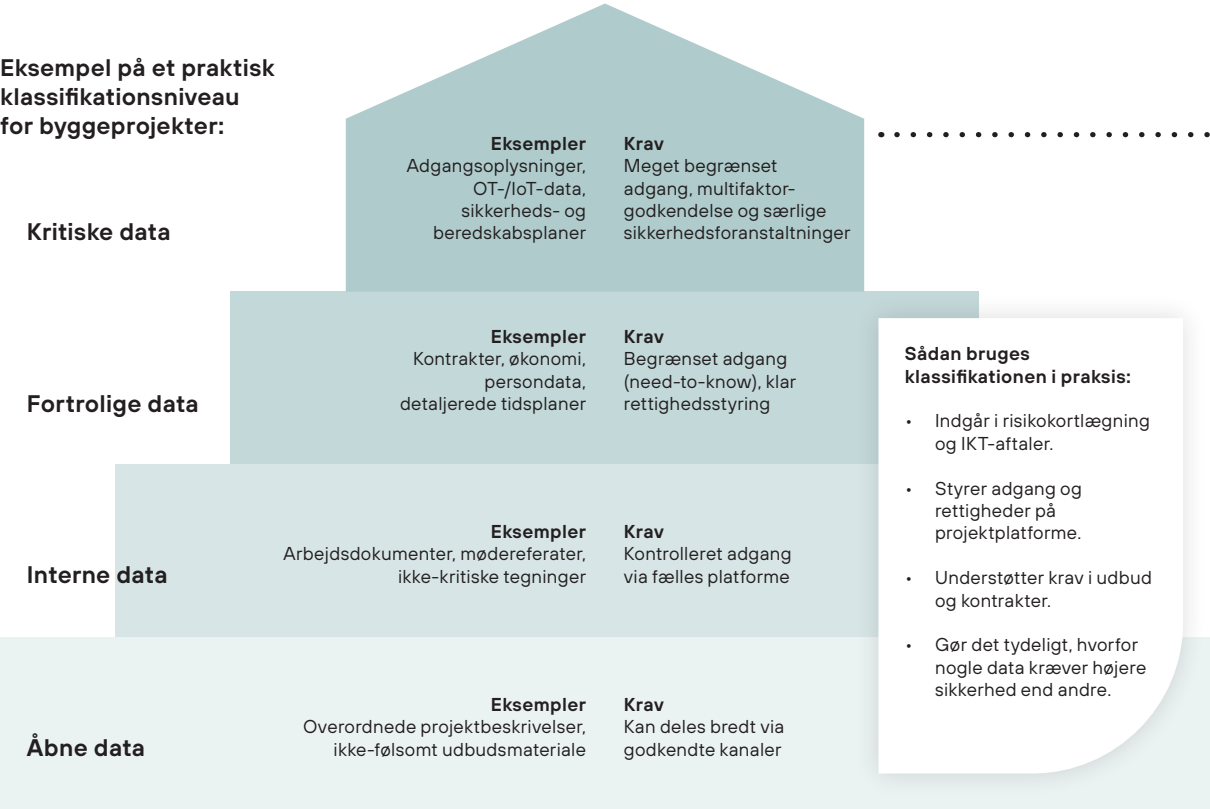
Ikke al data er lige kritisk – og derfor bør den heller ikke behandles ens.

I bygge- og anlægsprojekter deles store mængder data på tværs af virksomheder, systemer og faser. En enkel fælles data-klassifikation gør det muligt at prioritere sikkerheden dér, hvor konsekvenserne ved et brud er størst, og skabe fælles forståelse for adgang og deling.

Sådan bruges klassifikationen i praksis:

- Indgår i risikokortlægning og IKT-aftaler.
- Styrer adgang og rettigheder på projektplatforme.
- Understøtter krav i udbud og kontrakter.
- Gør det tydeligt, hvorfor nogle data kræver højere sikkerhed end andre.

Eksempel på et praktisk klassifikationsniveau for byggeprojekter:



4.7

Krav om digital sikkerhed

Virksomheder skal være opmærksomme på både lovkrav og de krav, bygherrer/investorer med fordel kan stille tidligt i processen, fx i udbudsmateriale og kontrakter.

Her er de mest centrale lovkrav og regler, byggeriets virksomheder skal kende til og navigere efter.

Lovkrav om sikkerhed (NIS2)

NIS2-loven¹² stiller krav til virksomheder om risikostyring, beredskabsplaner, dokumentation, træning og rapportering af cyberhændelser, indenfor kritiske områder.

Det juridiske ansvar ligger hos ejeren af byggeriet, hvilket oftest vil være bygherren. Men NIS2-loven har afledte konsekvenser ned gennem hele værdikæden. Store virksomheder skal sikre, at deres samarbejdspartnere efterlever relevante

krav. Det betyder, at rådgivere og entreprenører også forventes at leve op til kravene. Og kravene vil også kunne mærkes hos mindre virksomheder, fx underentreprenører, leverandører og i sidste ende også mindre håndværksvirksomheder.

NIS2 er risikobaseret: kritiske leverandører mødes af skærpede krav, mens ikke-kritiske leverandører typisk vil mødes af færre krav. Hvilke krav der gælder, vil derfor variere på tværs af projekter og leverandørroller.

AB-systemet

Virksomhederne skal også være opmærksomme på deres ansvar i AB-systemet, som omfatter standardvilkår for entreprisekontrakter. Hvis en cyberhændelse eksempelvis medfører forsinkelser, meromkostninger eller driftsstop, kan regler om tidsfristforlængelse, forsinkelsesansvar, mangler, ansvarsbegrænsninger m.v. blive relevante.



¹² samsik.dk/nis2/hvad-er-nis-2/

Krav i udbud

Cybersikkerhed bliver i stigende grad en del af udbud, hvor bygherrer kan stille krav om bestemte digitale platforme, samarbejdsformer og dokumentation af sikkerhed. Det påvirker ikke kun hovedaktører, men også underentreprenører og leverandører, og gør cybersikkerhed til et konkurrenceparameter.

■ *I større opgaver vi byder på, ser vi i stigende grad krav til hvilke digitale platforme, der skal bruges i samarbejder, og at vores medarbejdere har den rette træning. Det giver god mening, for det handler i sidste ende om at sikre, at vi samarbejder på en måde, der bygger på sund fornuft.*

Kenneth Højbjerg
Digital Lead hos AFRY, og deltager i projektets workshops

Cybersikkerhed i kontrakter

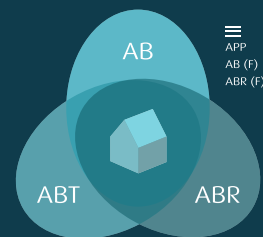
Cybersikkerhed bør tænkes ind i kontrakter fra start gennem risikovurdering, klare krav og afbalancerede sanktioner. Kontrakten bør understøtte samarbejde og ansvar – ikke blot være et konfliktværktøj.

■ *Cybersikkerhed ikke kun er et teknisk spørgsmål, men også et kontraktuelt og forretningsmæssigt emne. Mange nuværende aftaler i byggeriet regulerer ikke cybersikkerhed, hvilket kan skabe problemer, hvis nu et cyberangreb fører til forsinkelser, datamanipulation eller driftsstop. I de tilfælde kan rådgivere, entreprenører og leverandører blive økonomisk ansvarlige, også selvom de ikke er direkte omfattet af NIS2.*

Nicolaus Falk-Scheibel
Ph.D og advocat hos Molt Wengel

Almindelige betingelser i bygge- og anlægsvirksomhed

Betænkning nr. 1570
2018





4.8

Standarder og tilgange der er relevante for det digitale samarbejde

- **ISO 27001:**
Ramme for styring af informationssikkerhed
- **ISO 19650:**
Informationssikkerhed i tværfaglige projektsamarbejder, målrettet byggebranchen
- **Risikoanalyse og Business Impact Assessment (BIA)** som metode til prioritering af sikkerhed i projektering



- ■■ *Standardens logik kan bruges som et styringsredskab for hele projektets livscyklus – fra planlægning til drift. ISO 19650-5 skal ikke ses som et teknisk dokument, men som en fælles metode til at arbejde risikobaseret og helhedsorienteret med informationssikkerhed.*

Peter Bo Olsen
Standardiseringsspecialist, BuildingSMART Danmark

Styringsredskab med ISO 19650

ISO 19650 har fokus på samarbejde på tværs af organisationer og gør det muligt at etablere fælles processer, der kan genbruges og løfte branchen. Standarden angiver, hvilke processer, der bør gennemføres, i hvilken rækkefølge og med hvilket formål, og kan dermed fungere som et praktisk styringsredskab i projektarbejdet.

Informations- og kommunikationsteknologi (IKT)

IKT dækker over teknologi, der gør det muligt for byggeprojektets brugere at til få adgang til, redigere, overføre og gemme information.

IKT-bekendtgørelserne stiller krav til bl.a. IKT-koordinering, digital kommunikation, projektweb og digitale leverancer ved aflevering. Bygherren skal sikre koordinering af IKT-anvendelsen mellem alle parter gennem hele byggesagen.

IKT-aftaler kan udvides med cybersikkerhedskrav, ansvar/roller, procedurer, governance, risikokortlægning samt løbende opfølgning.

Da der er en del ansvar forbundet IKT-koordineringen, er det en god idé at knytte opgaven til en specifik person, altså til en IKT-koordinator eller en IKT-leder.

- ■■ *Formålet med IKT-bekendtgørelserne er at sikre en harmoniseret og værdiskabende anvendelse af IKT i bygge-, renoverings-, drifts- og vedligeholdelsesopgaver i den offentlige sektor. Produktiviteten inden for disse opgaver kan nemlig forøges væsentligt ved udvidet brug af IKT. Og det er et oplagt værktøj at bygge konkrete aftaler og fælles processer om sikkert digitalt samarbejde ind i.*

Allan Schiøtz
Produktchef for IKT i Molio

4.9

Tilgængelige værktøjer

Der findes en række værktøjer, virksomheder i byggebranchen kan tage ned fra hylderne og implementere for at øge den digitale sikkerhed i deres egen virksomhed og deres digitale samarbejder. Her er samlet nogle af de værktøjer.

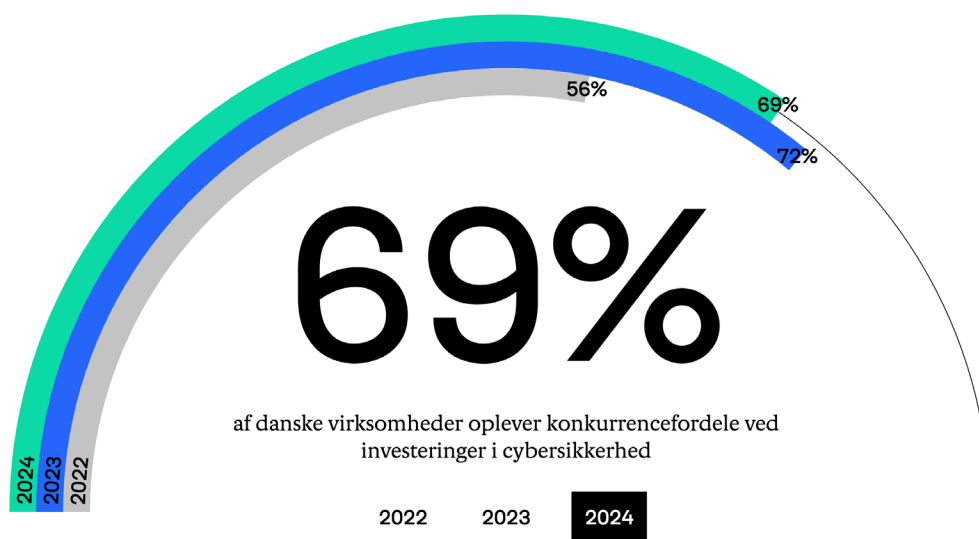


Industriens Fonds Cyberbarometer¹³

Selvevaluering og benchmark mod branchen giver anbefalinger til forbedringer inden for cybersikkerhed. Anbefalingerne er udviklet på baggrund af generel viden, ekspertinddragelse, caseinterviews mv.

D-mærkets selvevaluering¹⁴

Overblik over vigtige indsatsområder for it-sikkerhed og ansvarlig dataanvendelse. Processen er designet til effektiv dokumentation, og succeskriteriet for tilsynsprocessen er, at virksomheden ender med at kunne dokumentere efterlevelse af kravene tildelt i selvevalueringen og kommer mere robust og ansvarlig ud på den anden side.



¹³ Cyberbenchmark | Cybersikkerhed, Industriens Fond

¹⁴ ConTech Lab Cyber Survey 2026

Sikkerdigital.dk

Indeholder awareness-materialer og guides fra Styrelsen for Samfundssikkerhed inklusive Flyer med de 7 råd om it-sikkerhed, Flyer med 3 råd til sikring af IoT-enheder (smartprodukter) samt Bestyrelsens guide og tjekliste til digital ansvarlighed.



Vejledninger om cybersikkerhed

Der er udgivet en række vejledninger til virksomheder om deres cybersikkerhed, bl.a. hos Styrelsen for Samfundssikkerhed, Rådet for Digital Sikkerhed, Dansk industri, Digitaliseringsstyrelsen, Trafikstyrelsen og ISO.



Håndtering af sikkerheds- hændelser og beredskab i byggeprojekter:

Hvad gør vi, hvis det går galt?

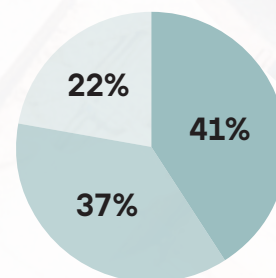
I bygge- og anlægsprojekter er tidsplaner stramme, afhængighederne mange, og samarbejdet ofte midlertidigt.

Når en digital sikkerhedshændelse opstår kan konsekvenserne hurtigt sprede sig på tværs af virksomheder og stoppe arbejdet på byggepladsen. Alligevel er beredskab ofte uklart:

1. Hvem tager ledelsen?
2. Hvem kontakter platformleverandøren?
3. Skal arbejdet stoppes – og hvordan fortsætter projektet midlertidigt?

Findes der en fælles procedure for håndtering af cyberhændelser eller databrud i projekter eller på byggepladsen?

- Nej, der er ingen fælles plan
- Delvist, men kun internt i vores egen virksomhed
- Ja, med klare roller og kommunikationsveje



Uden fælles aftaler risikerer projekter at miste både tid, data og tillid.

Data fra ConTech Labs Cyber Survey 2026 viser, at der sjældent findes en fælles procedure for håndtering af cyberhændelser eller databrud i projekter eller på byggepladsen.

Et enkelt og fælles beredskab gør det muligt at reagere hurtigt, begrænse skader og genoptage samarbejdet på en kontrolleret måde.



Hvad er en sikkerhedshændelse i byggeriet?

I byggeprojekter kan sikkerhedshændelser fx være:

- Kompromittering af brugerkonti (phishing, stjålne login-oplysninger)
- Uautoriseret adgang til projektplatforme eller mapper
- Utilsigtet deling eller læk af tegninger, modeller eller kontraktdata
- Ransomware eller nedbrud på centrale systemer
- Hændelser relateret til OT eller byggepladsens netværk

Ikke alle hændelser er lige alvorlige, men alle bør håndteres systematisk.



Et "light"-beredskab til byggeprojekter

Beredskabet skal være enkelt nok til at fungere i praksis og fælles for alle projektdeltagere. Et grundlæggende beredsskab kan bestå af flere forskellige elementer, og nedenstående er eksempler til inspiration:

1 Klare roller og kontaktpunkter

- Én ansvarlig for digital sikkerhed på projektet (fx IKT-koordinator).
- Kontaktoplysninger på platform-leverandør og evt. IT-drift.
- Klar beslutningskompetence ved hændelser.

3 Fælles reaktionsprincipper ved mistanke om en hændelse

- Stop yderligere spredning (luk conti, ændr adgangskoder).
- Informér relevante parter hurtigt og koordineret.

2 Midlertidig videreførelse af arbejdet

- Aftale om, hvordan kritiske informationer kan tilgås midlertidigt.
- Overvejelser om offline-adgang eller alternative løsninger.
- Prioritering af, hvilke funktioner der er mest kritiske for fremdrift.

4 Dokumentation og læring

- Kort registrering af hændelsen, forløb og konsekvenser.
- Vurdering af behov for justering af procedurer, adgange eller træning.

6.0

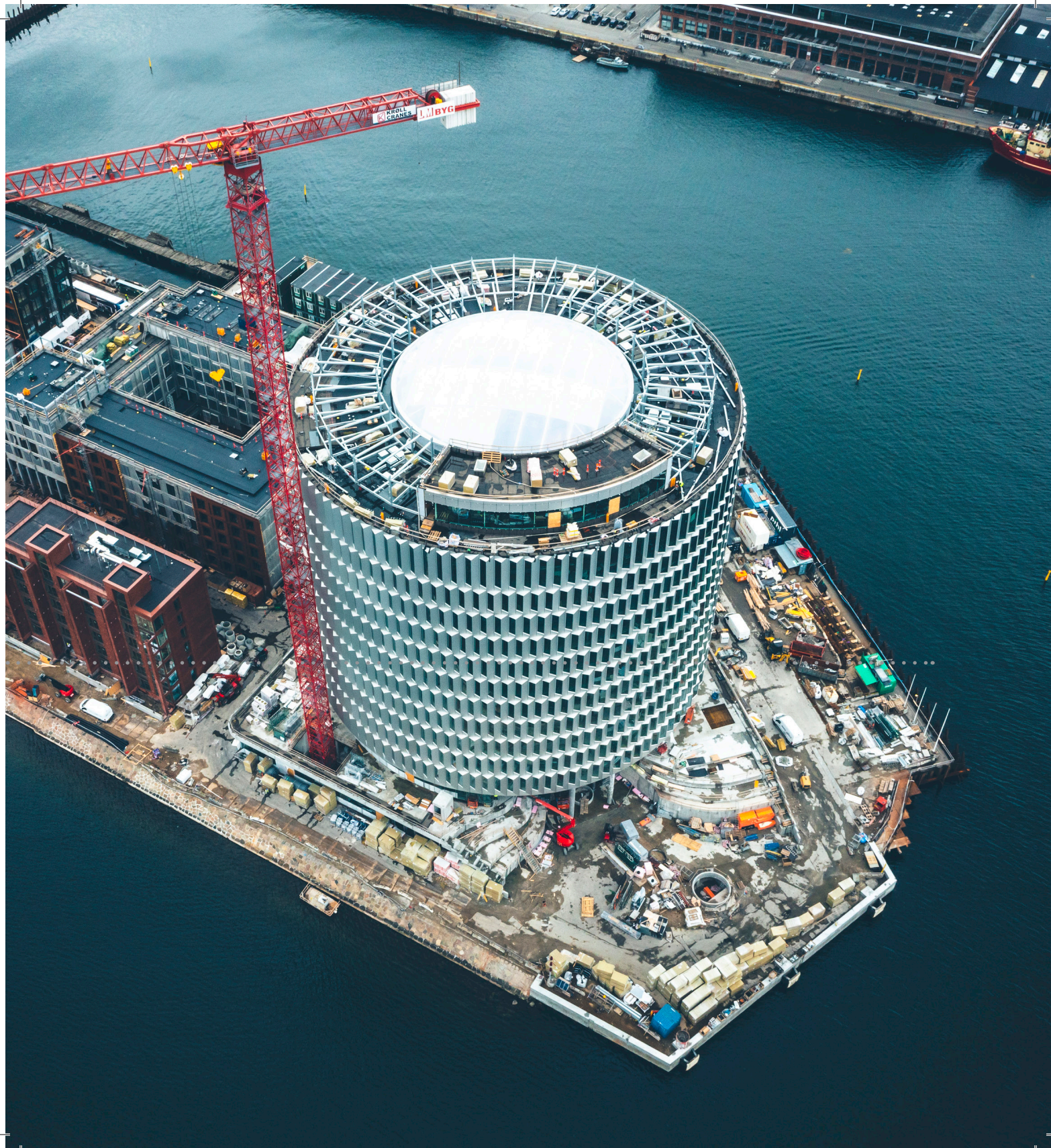
Hvilke løsninger mangler byggebranchen?

Der er endnu ikke etableret fælles metoder for sikkert digitalt samarbejde, hvor mange virksomheder arbejder sammen i samme projekt. Det gør det særligt svært for mindre virksomheder at navigere i krav og forventninger, og kan betyde, at de mødes af forskellige krav fra forskellige kunder.

■ ■ En mindre virksomhed kan ende med at skulle leve op til mange forskellige krav afhængigt af, hvem de samarbejder med. I projektet er der flere gange peget på, at der er behov for at udvikle fælles metoder og værktøjer, som kan hjælpe branchen med at operationalisere sikkerhed i praksis.

Christina Juell-Sundbye
Projektchef i ConTech Lab









Fælles baseline for cybersikkerhed

En fælles baseline – et minimumsniveau for sikkerhed – vil gøre samarbejde på byggeprojekter enklere og mere ensartet.

Løsningen kunne minde om arbejdsmiljøkravene i branchen. De er ensartede og gør det nemt at vide, hvad der gælder. Cybersikkerhed bør tænkes på samme måde. Ikke som noget "ekstra", men som en integreret del af kvalitet og drift. Hvis branchen kan blive enige om et niveau, vil det være en stor fordel for byggeriets digitale samarbejde.

En "light"-version kan dække mindre kritiske byggeprojekter. Denne model kunne fx indeholde punkter som multifaktorgodkendelse, adgangsstyring, opdatering af systemer og backup af kritisk data, mens mere kritiske byggerier (fx infrastruktur) kræver skærpede krav.

Fælles kompetencer for branchen

Et fælles træningsprogram med grundmoduler til alle projektdeltagere kombineret med projekt – eller virksomhedsspecifikke moduler kan skabe et fælles udgangspunkt.

Mange entreprenører og rådgivere bruger allerede lignende systemer til arbejdsmiljø og sikkerhed på byggepladsen, og cybersikkerhed kunne tænkes ind på samme måde.



Tjeklister

Hvad kan den enkelte virksomhed gøre?

- Gennemfør modenhedsvurdering.
- Etabler awareness-træning og kampagner.
- Indfør multifaktorgodkendelse på alle relevante systemer.
- Styrk adgangsstyring på netværk og systemer.
- Sikr løbende opdatering af software og enheder.

Hvad kan byggeprojektet gøre? De mest håndgribelige løsninger handler om:

- Multifaktorgodkendelse.
- Adgangsstyring.
- Sikre netværk og segmentering.
- IoT/OT-sikring.

Samtidig er fælles rammer afgørende:

Sikkerhed skal ind i projektets kultur, struktur og samarbejdsmodel. Projektet kan stille dokumentationskrav om modenhed og sikkerhedsforanstaltninger.

Centrale greb i byggeprojektet:

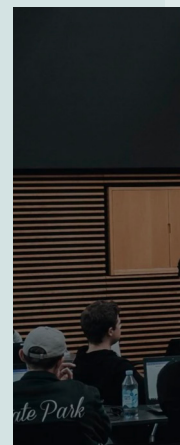
- Risikokortlægning for projekt og byggeplads, opdateret løbende og med klar prioritering.
- IKT-aftaler, der definerer ansvar, roller og governance.
- Løbende opfølgning og træning, inkl. procedurer og beredskab, der kan dokumenteres og opdateres.

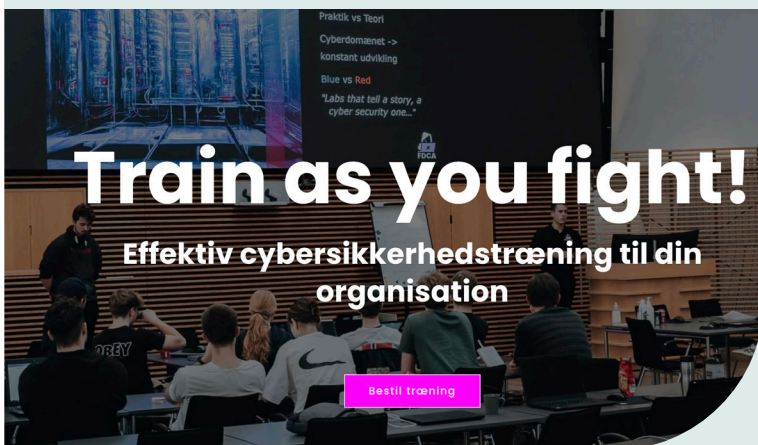
8.0

Digitale løsninger du skal holde øje med

Det digitale sikkerhedsområde udvikler sig konstant, og det kan være en fordel at holde øje med digitale løsninger og virksomheder, der løbende kommer ind på markedet.

Her præsenteres en række udvalgte løsninger, der adresserer forskellige behov. Der er tale om eksempler på løsninger der findes, og skal dermed ikke læses som konkrete anbefalinger.





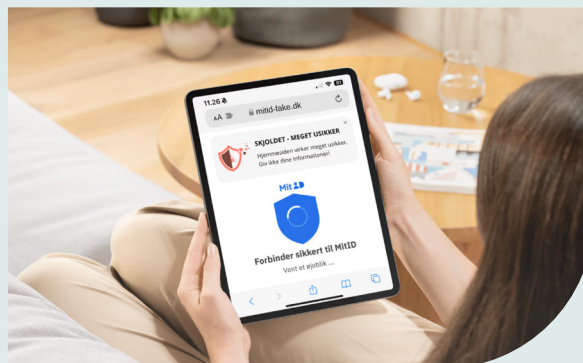
SagaLabs



SagaLabs er en hurtigt voksende startup, der tilbyder realistisk cybersikkerhedstræning med mantraet 'Train as you fight'. I deres selvudviklede træningsplatform træner alt fra virksomheder til myndigheder i virkelighedsnære scenariebaserede angreb som ransomware, insider leaks og phishing.

Træningen er instruktørledt ved brug af fagfolk fra cyberfrontlinjen, som sikrer en god hands-on læring, samt at øvelserne er virkelighedsnære og up to date.

SagaLabs udspringer af erfarne kræfter fra Forsvaret med rødder i cybersikkerhed og softwareudvikling. De kombinerer teknisk indsigt med pædagogisk styrke og hjælper virksomheder og myndigheder med at opbygge et stærkt og praktisk forankret cyberberedskab.



Skjoldet



SKJOLDDET er den proaktive forsvarslinje, der advarer mod svindel, gennem et simpelt visuelt "stopskilt", før man bliver snydt.

Skjoldet betnytter en proaktiv kunstig intelligens og algoritme baseret detektion, som beskytter og advarer i realtid – mod phishing, falske konkurrencer, falske webshops og andet scam – direkte på den side man besøger, også selvom truslen ikke tidligere er kendt.

SKJOLDDET kan tages med på farten, da det er en browserudvidelse til alle enheder og browsere. For private er det helt anonymt og gennem organisationsbeskyttelse kan du også se, hvis dine medarbejdere rammes af svindel.

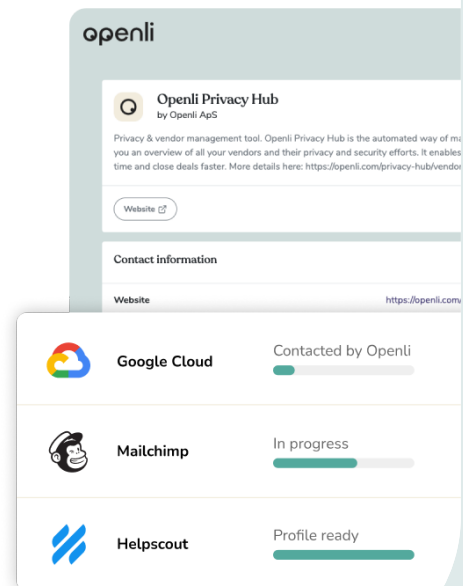
Kriminelle bliver hele tiden dygtigere, men med SKJOLDDET kan brugeren på få sekunder se, om en side er falsk.

Det, der gør SKJOLDDET unikt, er, hvor proaktivt det beskytter brugeren ved at levere advarsler i realtid direkte på hjemmesiden, inden man får skrevet oplysninger ind.



Privacy & AI Compliance made easy!

Openli is the automated way of managing your vendors, scaling your privacy efforts and building trust. Loved by customers for being easy to use.



Openli

Openli tilbyder hjælp til at screene leverandører og digitalt administrere virksomhedens privatlivsindstillinger.

Virksomheden har også fokus på ROPA'en, som er "record of processing activities", som er et GDPR krav, og består af en dokumenteret liste over virksomhedens data aktiviteter.

Cyber Security Tool

Erhvervshus Hovedstaden (EHHS) tilbyder små og mellemstore virksomheder i byggeriet et "CyberTjek". Gennem en række indledende spørgsmål afdækkes virksomhedens risikoprofil i forhold til dens værdikæde.

Formålet er at give et klart billede af, hvor virksomheden står, og hvilke områder der kræver opmærksomhed. Derudover tilbyder EHHS 1:1-samtaler, hvor virksomhederne får konkret vejledning om, hvordan de bedst sikrer sig mod cyberangreb.

Cybersikkerheds Tool

Dit værktøj til at måle, forstå og forbedre din virksomheds cybersikkerhed.



Erhvervshusene

1 — 2 — 3 — 4 — 5

Virksomhedsoprettelse

Vælg erhvervshus og indtast CVR for at oprette din virksomhed

Virksomhed

Vælg erhvervshus du er tilknyttet

CVR

Næste

Afrunding

Digitalisering af byggebranchen er et vigtigt redskab til at rykke branchen i en mere effektiv og bæredygtig retning. Derfor har forudsætningen i denne udgivelse også været, at arbejdet med digitalisering skal gøres mere sikkert – ikke minimeres.

Denne publikation har således beskrevet byggeriets særlige sårbarheder og peget på konkrete greb, der kan understøtte sikkert digitalt samarbejde i praksis. Det handler ikke om at gøre alting lige sikkert, men om at arbejde risikobaseret og proportionelt, med fokus på det, der er mest kritisk for projektets fremdrift, sikkerhed og tillid.

Sikkert digitalt samarbejde bør betragtes på linje med arbejdsmiljø og kvalitet: som en integreret del af professionel projektledelse og godt samarbejde. Ved at tænke digital sikkerhed ind tidligt, skabe klarhed om ansvar, arbejde systematisk med adgang, data og beredskab og investere i kompetencer og kultur kan byggebranchen reducere risiko og samtidig styrke produktivitet og samarbejde.

Projektet "Sikkert digitalt samarbejde i byggeriet" er et skridt mod fælles metoder og værktøjer for branchen. Det næste skridt er at omsætte principperne til handling i konkrete projekter og forankre dem i samarbejdet på tværs af værdikæden. Når digital sikkerhed bliver en fælles praksis, styrkes både tilliden, robustheden og kvaliteten i fremtidens byggeri.







Ordliste

BYOD

Bring Your Own Device

CDE

Common Data Environment (fælles datamiljø)

CER

Critical Entities Resilience - EU-regulering, der stiller krav til robusthed og modstandsdygtighed hos virksomheder og organisationer, som leverer eller understøtter kritiske samfuntsfunktioner.

Cybersikkerhed

Cybersikkerhed dækker i publikationen over it-sikkerhed for netværksforbundne it-systemer, som defineret af Styrelsen for Samfundssikkerhed (SAMSIK)¹⁵. Cybersikkerhed udgør en del af den bredere betegnelse informationssikkerhed.

DoS

Denial of Service - et angreb, hvor et system eller en digital tjeneste overbelastes, så den bliver utilgængelig for legitime brugere.

Hardening

Sikkerhedsoptimering af software

Informationssikkerhed

Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger, som opsættes for at sikre informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed. I arbejdet indgår blandt andet organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer for behandling af data, styring af leverandører samt tekniske sikringsforanstaltninger.

IoT

Internet of Things

IT-sikkerhed

IT-sikkerhed handler om at beskytter information, der behandles i it-systemer (hardware og software) mod uautoriseret adgang, brug eller ændring¹⁶.

Legacy-systemer

Forældede systemer

MDM

Mobile Device Management: en IT-løsning, som man bruger til at administrere og sikre smartphones, tablets og bærbare computere, der bruges til arbejde.

MFA

Multi-Factor Authentication (multifaktorgodkendelse): betyder, at du skal bekræfte din identitet på mere end én måde, når du logger ind et sted.

OT

Operational Technology, som fx kraner

Ransomware

En type cyberangreb, hvor data eller systemer låses eller krypteres, og der kræves løsepenge for at genskabe adgangen.

¹⁵ Ordforklaringer – centrale begreber i cybersikkerhed (A-Å)

¹⁶ Hvad er informationssikkerhed? – SKI

CON
TECH
LAB_

INDUSTRIENS FOND



KNUD HØJGAARDS FOND

RAMBØLL
FONDEN

MOLIO
— viden, du bygger på

ConTech Lab er byggebranchens fælles udviklingsplatform, hvor byggeriets virksomheder sammen kan udvikle og eksperimentere med nye måder at benytte data, digitalisering og teknologi på til at skabe fremtidens byggeri – et mere bæredygtigt og produktivt byggeri.

ConTech Lab deler al viden og læring, så det kommer hele branchen til gode.

.....
ConTechLab.dk

