

Beskytt adgangs-kontrollsystemene dine mot cybertrusler

Kraften i forebyggende vedlikehold



dormakaba

Det nye risikobildet

Adgangskontroll er en førstelinje i forsvaret mot cybertrusler

Moderne anlegg drives av et sammenkoblet nettverk av IT-systemer, operasjonell teknologi og smarte enheter. Adgangskontroll står i sentrum av dette nettverket, noe som gjør det stadig mer attraktivt for angripere som leter etter inngangsveier med lavere synlighet og svakere oppdateringsstyring.

Eldre enheter, utdaterte krypteringsmetoder og programvare (firmware) som ikke lenger støttes, kan skape strukturelle svakheter som strekker seg langt utover én enkelt dør. En kompromittert kontroller eller en feil vedlikeholdt leser kan eksponere sensitive personopplysninger, forstyrre driften eller gi tilgang til det bredere nettverket.

Regelverket har reagert deretter. GDPRs krav til «egnede tekniske tiltak» gjelder direkte for adgangssystemer som håndterer legitimasjonsdata, mens ISO 27001 og NIS2 vektlegger aktiv sårbarhetsstyring. Samsvar handler ikke lenger bare om konfigurasjon; det krever kontinuerlig, evidensbasert vedlikehold.



30%

år-til-år økning i cyberangrep som retter seg mot nettverkstilkoblede fysiske sikkerhetssystemer det siste året

Kilde:
https://ciosea.economictimes.indiatimes.com/news/security/critical-infrastructure-cyberattacks-increase-30-percent-in-one-year-report/112854335

Sikker adgang alltid oppdatert

Er adgangskontrollsystemet deres oppdatert og sikret?
Et adgangskontrollsystem er selve nøkkelen til sikker og effektiv drift av bygget ditt. Programvaren bak systemet må fungere feilfritt – hver dag. Med en vedlikeholdsavtale for denne programvaren sikrer du at løsningen alltid er oppdatert, stabil og klar til å møte nye krav.

Trygghet i hverdagen
- Regelmessige oppdateringer lukker kjente sikkerhetssårbarheter
- Kontinuerlig støtte for nye funksjoner og produkter
- Sikret kompatibilitet med:
  - servermiljøer
  - bredere IT-infrastruktur
- Redusert risiko for nedetid som påvirker:
  - sikkerhet
  - daglig drift og logistikk

Forutsigbare kostnader
- Faste og budsjetterbare vedlikeholdskostnader
- Redusert risiko for uventede reparasjonskostnader
- Tidlig oppdagelse reduserer risikoen og kostbare akutte tiltak.

Lengre levetid på investeringen
- Forbedret systemytelse gjennom regelmessig vedlikehold
- Lengre livssyklus for programvare og systemkomponenter
- Maksimer verdien av investeringen – år etter år

En serviceavtale er mer enn en forsikring:
- Det styrker aktivt sikkerheten
- Forbedrer den operative effektiviteten
- Opprettholder kontroll over systemets ytelse
- Sikrer pålitelig drift uten avbrudd

Serviceavtale som verktøy for NIS2-etterlevelse
Med innføringen av NIS2 (EUs nye direktiv for digital sikkerhet) stilles det tydelige krav til systematisk cybersikkerhetsarbeid, oppdateringsrutiner og dokumentert drift av digitale sikkerhetssystemer. En serviceavtale sikrer at adgangskontrollsystemets programvare oppdateres kontinuerlig, og at kjente sårbarheter håndteres raskt.



Hvordan påvirkes kommuner og offentlig sektor?

Kommuner forvalter verdier, personopplysninger og samfunnskritiske funksjoner som må beskyttes døgnet rundt. Med NIS2 stilles det krav til dokumentert risikostyring, løpende oppdatering av digitale sikkerhetssystemer og tydelig leverandøroppfølging.

En vedlikeholdsavtale for adgangskontroll sikrer at programvaren kan holdes oppdatert, at sårbarheter lukkes raskt og at alle endringer er sporbare.
Dette bidrar til å forhindre uautorisert adgang og fungerer som et praktisk verktøy for å ivareta innbyggernes sikkerhet, beskytte personopplysninger og oppfylle NIS2-kravene på en forutsigbar og kostnadseffektiv måte.



Hvordan påvirkes eiendom og byggforvaltning?

Moderne bygg er digitale økosystemer der adgangskontroll er en kritisk sikkerhetsfunksjon. NIS2 gjør det nødvendig å behandle disse systemene som en del av virksomhetens cybersikkerhet.

Med vedlikeholdsavtale sikres jevnlige oppdateringer, kompatibilitet med øvrige tekniske anlegg og dokumentert håndtering av sårbarheter.
Dette gir gårdeier og forvalter kontroll på hvem som har adgang, hvordan systemet driftes, og at krav til sporbarhet og leverandøroppfølging ivaretas.

Resultatet er tryggere bygg, mer stabile leieforhold og etterlevelse av nye regulatoriske krav uten uforutsette kostnader.

Hvordan påvirkes industri og kritisk infrastruktur?

For industri- og infrastrukturselskaper kan et avbrudd i adgangskontrollen stoppe produksjon, svekke HMS og true forsyningssikkerheten. NIS2 krever at virksomheten har kontroll på digitale sårbarheter, oppdateringsregime og beredskap mot cyberhendelser.

En vedlikeholdsavtale sørger for kontinuerlig patching, kvalitetssikrede oppgraderinger og rask tilgang til spesialkompetanse når noe skjer. Dette reduserer risikoen for uautorisert tilgang til systemet, driftsstans og brudd på myndighetskrav. Avtalen gir også dokumentasjon på forsvarlig drift – et sentralt element i å oppfylle NIS2-krav til robusthet og kontinuitet.

Helhetlig sikkerhet gjennom kombinert vedlikeholds- og serviceavtale

Adgangskontroll fungerer best når både programvare og fysiske komponenter vedlikeholdes samlet. Med en kombinert vedlikeholds- og serviceavtale sikres oppdaterte systemer, stabile løsninger og velfungerende utstyr – før feil utvikler seg til driftsstans eller sikkerhetsbrudd.

Som produsent anbefaler dormakaba service gjennom autorisert Partner for korrekt håndtering av hele løsningen. Resultatet er lengre levetid, færre uforutsette kostnader og dokumentert sikker drift i tråd med krav til internkontroll og NIS2.

Oppdag et unikt
utvalg













Access Automation Solutions

Access Control Solutions

Access Hardware Solutions

Services

EAD_BRO_SoftwareMaintenance_NO_0001470_01
Med forbehold om tekniske modifikasjoner uten forvarsel

dormakaba.com

dormakaba Norge AS
Tlf.: 06866
firmapost.no@dormakaba.com
www.dormakaba.no