WHITEPAPER

Så höjer du säkerheten i era fastigheter

advania

Innehåll

Introduktion

Digitaliseringen har pågått länge, men just de senaste åren har utvecklingen eskalerat. De som blir duktiga på att digitalisera får därmed en fördel gentemot andra.

Den allt mer krävande fastighetsbranschen, kombinerad med hur vi köper och nyttjar IT och dess funktioner, gör att det sätts en enorm press på fastighetsbolagen. Om du inte digitaliserar nu, kommer det inte att fungera sen.

Detta gör att många riskerar att ta snabba och ogenomtänkta beslut. Man fokuserar på en ny IT-lösning, funktionen och tjänsten i sig – men glömmer bort andra saker – somsäkerheten.

I den här guiden berättar vi både om de positiva aspekterna och utmaningarna kring dagens dig taliserade fastigheter och molnet, samttipsar om hur du som exempelvis arbetar som IT-chef, CIO, CDO, teknikchef eller besitter en annan, liknande hög chefsposition, bemöter och hanterar dessa utmaningar. Dette er en digitaliseringsguide för dig som är verksam inom bygg- och fastighets-branschen och tycker säkerhet är viktigt.

Trevlig läsning önskar,
Team Advania

Positiva aspekter som digitaliseringen av fastigheter medför

Du möjliggör för en mer klimatsmart miljö

En av de allra starkaste drivkrafterna gällande digitaliseringen av fastighetsbranschen är hållbar het. Digitaliseringen fungerar som en möjliggörare för en mer hållbar värld, och just molnets ökande betydelse har spelat en stor roll i fastighetsdigitaliseringen.

Du tillgodoser hyresgästernas önskningar

Inom fastighetsbranschen har alltid hyresgästernas krav och behov varit i centrum. Digitaliseringen kan erbjuda enkla vägar att tillgodose deras behov samtidigt som du kan öka fastighetens omsättning och höja fastighetens värde.

Det kan handla om allt från digitala assistenter till appar som möjliggör en smidigare kommunikation för hyresgästerna, eller möjligheten att erbjuda smarta molnbaserade lösningar för aktivitetsbaserade kontor.

Du kan spara pengar

Digitaliseringen har också medfört att det blivit lättare att få en tydlig bild av hela fastighetsdriften, vilket kan leda till att fastigheten kan sänka sin energianvändning och hela driftkostnaden.

Implementeringen av olika tekniska lösningar kan också resultera i mer tid över för fastighetsskötarna att arbeta med mer värdeskapande arbetsuppgifter.

En av de största säkerhetsutmaningarna idag är molnet

Trots alla fördelar med digitaliseringen och att lägga över sin drift i molnet så kan det även vara riskabelt ur såväl en säkerhets- och integritetsaspekt. I vårt moderna samhälle har hackare inte längre något behov av en fysisk enhet att arbeta med. Förr stal de kanske en känd persons telefon eller dator – idag hackas exempelvis istället deras iCloud-konto där allt finns samlat.

I en molnplattform finner man alla företagets kunder. Det vill säga, om ett globalt teknikföretags molntjänst skulle utsättas för intrång kan hackare komma åt allting som rör företaget därifrån. Ju mer det centraliseras, desto mer attraktivt blir det för en hackare.

Internet of Things – en problematisk sida avmolnet

Allt ska kopplas upp mot molnet, och en rad prylar, så kallade Internet of Things (IoT) är idag online, som kyl- och värmesystem. Det innebär bland annat att fastighetsskötare eller annan personal enkelt kan säkerställa att värmen ligger på rätt temperatur och hålla koll så att det exempelvis inte finns någon vattenläcka i fastigheten.

Men att vara konstant uppkopplad innebär också att det för en hackare kan bli lättare att hacka en smart pryl, och därmed få tillgång till exempelvis ditt värmesystem.

Vi har de senaste åren bland annat läst om hackare som lyckats nå ett kasino-system genom att ta sig in via ett oskyddat akvarium. Och även hur kylsystem legat helt öppna mot internet då man glömt att byta sitt standardlösenord. Incidenter som tydligt visat hur enkelt det är att utsättas för intrång och på molnets sårbarhet.

Ett bra tips

Kravställ din leverantör av molntjänster. Säkerställ att ett tydligt säkerhetstänk finns med från första början och att det är något företaget prioriterar.

Lösningen bygger på att systemet åtskiljs

Att säkerställa att man kontinuerligt byter ett standardlösenord måste bli en självklarhet för alla inom verksamheten. Det får varken bli något som skjuts upp eller bara glöms bort. Löpande lösenordsbyte är viktigt, men än viktigare är användandet av komplexa lösenord. Det bästa är att använda sig av lösenfraser som är mer än 14 tecken för optimal säkerhet. Se även till att ha som standard att alltid ha tvåfaktorsautentisering på alla inloggningar till era viktiga system.

Vad man vidare måste göra när det gäller IoT är att se till att ansluta dessa smarta prylar på segment som bara är uppkopplat mot andra smarta prylar – inte mot större säkerhetssystem och liknande. Man bör även använda säkra kommunikationsprotokoll när det gäller radiobaserad kommunikation. Det kanske är okej att själva akvariet är öppet mot internet, men om någon tar sig in ska de inte komma åt andra kritiska system.

Vem som har access till vad blir allt viktigare

Känner du som fastighetsägare ens till samtliga personer som har access till fastigheten idag? Minns du exempelvis alla installationsfirmor som har varit inblandade under åren? Se inledningsvis över vilka som har access och om dessa personer verkligen fortfarande behöver ha tillgång till fastigheten.

Kontrollera också vilka specifika personer som har access till olika system i fastigheten, samt fysisk access till vilka platser. Säg att en leverantör eller en anställd på företag har access till ett system, men så avslutas samarbetet. Då glömmer man ofta att ta bort behörigheten – vilket givetvis är en säkerhetsrisk då personen fortfarande kommer åt era system. En anställd använder i regel en mängd olika konton, och det kan därmed vara svårt att komma ihåg att koppla bort personen från samtliga av dessa.

Ett bra tips

Inrätta rutiner för hur ni avslutar en persons access när ett samarbete avslutas, och ge hellre specifik access till en applikation än till hela nätverket. Om det sker personalförändringar hos en underleverantör, säkerställ också att de byter lösenord på samtliga sina inloggningar.

Redan idag finns lösningar för att hantera problematiken kring access i fastigheter, och vi kommer att se fler i framtiden. Det kan handla om plattformar där man erbjuder inpassering och säkerställer vem eller vilka som ska ha tillgång till olika delar i en fastighet.

Detta kan exempelvis möjliggöras genom att man identifierar sig med BankID och då erhåller en personlig digital nyckel som ger access i fastigheten.

Ransomware-attacker förekommer också allt mer

Förr hackade man för att gå in och förstöra. Nu är det i första hand ekonomiska brottslingar som härjar, som istället tjänar pengar på att sälja den data de kommer åt, eller utöva utpressning. Allt fler företag har upplevt hur det känns att bli tagen som gisslan när hackare krypterat deras information. Säg exempelvis att en persondator på ett större företag blir infekterad av ransomware. Detta kan sedan om man har otur spridas till samtliga av företagets 10 000 datorer.

Dessa kan i sin tur smitta alla andra klienter, och så fort man fixar servrarna där all data befinner sig så smittas de ner igen av alla klienterna. Självklart vill man inte betala för att komma ur knipan – men många har inte råd att istället betala vad som krävs för att installera om samtliga datorer, så man tvingas ändå betala hackern.

Detta kan givetvis få förödande konsekvenser för fastigheter. Säg att en fastighet blir utsatt för en ransomware-attack när det är tolv minusgrader ute. Om fastigheten utsätts för hot om avstängning av värmen – har man något annat alternativ än att betala?

Några sätt att hantera ransomware

- Segmentera näten så att system som är öppna motinternet ej når kritiska funktioner
- Använd starka lösenfraser och byt demofta
- Aktivera Nätverksåtkomstskydd
- Uppdatera alltid Malware Remover till den senaste versionen

Så kan Advania hjälpa ditt företag att få digitalisering och säkerhet att mötas

Fastigheter är uppkopplade idag, och kommer att fortsätta att vara det. Man måste därför koppla upp fastigheterna på ett säkert, kontrollerat sätt – något vi på Advania hjälpt fastighetsbolag med i drygt 15 år.

Möter du säkerhetsutmaningar i fastigheten som du inte vet hur du ska hantera? Är du nyfiken på att centralisera era lokala system och därigenom öka säkerheten? Vill du addera tjänster åt hyresgästerna för att på så sätt öka värdet på fastigheten?

Fastighetsbolag besitter kompetensen och mängder av idéer, men har sällan tillräckligt med resurser som faktiskt kan tillbringa tid ute i fastigheterna. På Advania har vi expertisen inom IT och säkerhet samt resurser och infrastruktur och kan hjälpa till med en rad olika utmaningar. Vi kan vara med hela vägen och sköta accessen, både fysiskt och tekniskt i fastigheterna. Vi kan hjälpa till med upphandling av fastighetssystem genom hela processen och samla alla delar du behöver från olika leverantörer.

Intresserad av att veta mer om våra lösningar?

Kontakta oss

advania

Vi gör det enkelt att växa med IT

advania.se