Skolfastigheter i Stockholm AB

Strategier för digitalisering i fastighetsorganisationer

SISAB:s Arena 2020 – tema informationssäkerhet
Sammanställning av workshop

Läsanvisning

Den 13 februari 2020 var det dags för den tredje upplagan av SISAB:s arena om strategier för digitalisering och informationshantering. Detta år på temat informationssäkerhet.

På arenan presenterade talare från SISAB, KTH, Specialfastigheter och Stockholms stad.

I detta dokument har vi sammanställt frågeställningar utifrån de fyra olika teman som diskuterades under arenans workshop-del. Tillsammans med talarnas presentationer utgör det en dokumentation av dagen och underlag för SISAB:s och branschens vidare diskussioner.

Har du frågor om innehållet eller om arenan, kontakta SISAB:s informations-strateg Pouriya Parsanezhad, pouriya.parsanezhad@sisab.se.

Hotbilden mot fastighets-bolagen – hur ser den ut?

Den ökade informationsmängden och en ökad uppkoppling mot internet medför en ökad sårbarhet och vi ser fler och fler attacker även mot fastighets-organisationer och byggnader. Ofta beror sårbarheten på avsaknad av medvetenhet kring riskerna och att rutiner samt strategier saknas. Attackerna kan rikta sig mot styrsystem för el, värme, kyla eller ventilation men också mot system för passage och larm.

Integrerad uppkoppling kan innebära en risk för intrång, avlyssning, sabotage och avslöjande av hemliga uppgifter. Vägen som information strömmar ut kan även innebära en möjlig väg in. Det finns möjlighet att utläsa detaljer från byggnaden, som t ex: hur stor datakraft som finns installerad, om det finns särskilda verksamheter som laboratorier eller annan känslig verksamhet, hur många personer som rör sig i lokalerna.

Sammanfattning av diskussionerna

Det största hotet för fastighetsägare kan vara:

1. Medieförsörjning av el, värme, kyla och vatten.
2. Obehöriga som befinner sig på fel sida av ett skalskydd, fysiskt eller digitalt, och i och med det får tillgång till känslig information.
3. Vår egen okunskap/omedvetenhet, d.v.s. den mänskliga faktorn.
4. Ritningshantering – hur delar vi ut ritningar/modeller över våra byggnader och hur hanteras och används ritningarna/modellerna hos mottagaren?

Försök till intrång och överbelastningsattacker har hänt flera av de deltagande organisationerna. Antalet attacker är många men än så länge har inte någon allvarlig skada uppstått. Vid samtalet var alla eniga om att det är viktigt att dela med sig av vad som har inträffat för att kunna dra lärdomar och hjälpa varandra hur vi kan hantera attacker.

Förslag på åtgärder:

- Genomför regelbundna penetrationstester för att testa säkerheten.
- Använd separata nät för SCADA-lösningar.
- Utbilda personalen regelbundet, varje eller vartannat år.
- Dela kunskap med andra och inhämta erfarenheter.
- Ta hjälp av experter.

Informationsklassning av byggnadsinformation

Att koppla upp sina byggnader och utrusta dem med IoT kan ge ett övertag mot konkurrenter och vara ett effektivt besparingssätt. Risken finns dock att organisationen endast fokuserar på fördelarna med smarta lösningar och på så vis riskerar att bygga in problem för framtiden när det saknas kontroll över hur all information hanteras.

Alla leverantörer av intelligenta system och komponenter vill ge sig själv en möjlighet att ha ett informationsöverläge för att få ett försprång gentemot sina konkurrenter. Nya marknader uppkommer inte så ofta och informationskapitalism är fortfarande nytt. Det är naturligt att dessa företag samlar information från den utrustning de sålt. Om hyresgäster ställer krav på att veta vilken information som genereras i de lokaler de bedriver verksamhet och hur den hanteras, kan fastighetsägaren försäkra att de kan tillmötesgå kraven?

Sammanfattning av diskussionerna

Det finns en utmaning i att förstå innebörden av informationsklassning och vilka som är de avgörande frågorna. När vi exempelvis jobbar med ritningar och BIM-modeller som lämnas ut måste vi också skicka med säkerhetsstafettpinnen.

Om vi inte har kontroll på hur informationen hanteras externt spelar det ingen roll vad vi gör internt med rutiner, klassning, tillgänglighet etc.

Förslag på åtgärder:

- Utse informationsägare, informationsägarskap för olika informationsmängder är grunden.
- Analysera risker, sårbarheter och vad konsekvensen är om vi börjar tappa information eller det kommer in felaktig information i systemet.
- Genomför en detaljerad informationsklassning och beakta konfidentialitet, riktighet och tillgänglighet.
    - Konfidentialitet betyder att informationen är tillgänglig endast för de personer som har behörighet att ta del av den.
    - Riktighet betyder att innehållet i informationen ska vara korrekt och inte kunna förändras av obehöriga.
    - Tillgänglighet betyder att informationen ska vara nåbar när den behövs.

Smart stad – öppna data

Den smarta staden förutsätter tillgång till öppen data för att olika aktörer ska kunna interagera. Våra kunder och hyresgäster vill ha samma service och information från sin hyresvärd som man får från andra leverantörer inom till exempel e-handel och resetjänster. Man vill kunna ställa vilken fråga som helst, närsomhelst, i vilken kanal som helst och bli bemött i ett användarvänligt gränssnitt med ett informativt svar eller information om att en åtgärd är utförd.

Fokus är informationssäkerhetsperspektivet och det som behöver analyseras är avvägningen mellan öppen data (och mycket data) och informationssäkerhet i ett läge där vi ser en ökad hotbild och fler attacker mot våra olika IT-lösningar.

Sammanfattning av diskussionerna

Människan är en stor risk vid informationshantering och informationssäkerhet. Därför ska vi satsa på ”huret” d.v.s. hur information kan användas av riktiga människor i verkligheten.

Mycket delas redan då det finns en stor nytta i att dela data mellan organisationer. Det är kanske inte alltid vi själva som kommer på alla de nya smarta tjänsterna utan vi behöver tillgängliggöra öppna data för att andra ska komma upp med de innovativa lösningarna.

Det finns en risk att stora kommersiella aktörer tar över vår information och vår informationshantering. Som fastighetsägare måste vi ta kontroll över vår information och säkerställa att det finns strukturer för hur man ska jobba med informationen om våra fastigheter.

Förslag på åtgärder:

- Ta kontroll över informationen, utveckla informationsstrategier.
- Beakta nyttor (innovation m.m.) mot risker.
- Utbilda medarbetarna och skapa en medvetenhet i organisationen – människor.
- Beakta integritet mot privata aktörer.
- Skala av information, d.v.s. separera information som är känslig.

Hur agerar fastighets-bolagen?

Behovet av att kunna hantera den ökade informationsmängd som digitaliseringen medför ställer delvis helt nya krav på fastighetsbolagen. Kraften i att ha tillgång till information var och när den än behövs är tydlig men det kräver strategi, struktur och rutiner för att göra det möjligt.

Informationsägarskap, tillgänglighet, tillförlitlighet, säkerhet och sekretess blir centrala begrepp i informationshanteringen. Den fastighetsägare som tar fram verktyg och rutiner för att säkerställa den digitala säkerheten kan erbjuda något som i framtiden kommer vara nödvändigt. Det finns en stor risk att man annars redan nu bygger in något som kommer att bli dyrt och komplicerat att hantera.

Det finns ett antal frågor som måste beaktas:

- Vilka krav kan våra hyresgäster komma att ställa?
- Hur kan fastighetsägaren garantera att kraven uppfylls?
- Vilken typ av information skapas och samlas in som fastighetsägaren ansvarar för?
- Om hyresgäster ställer krav på att veta vilken information som skapas i de lokaler de bedriver verksamhet, hur kan då fastighetsägaren försäkra att de kan tillmötesgå och förmedla kravet vidare?

Hyresgästernas krav avseende kontroll av byggnadsrelaterad information kommer självklart att variera beroende på verksamhet och uppdrag. De flesta kan idag tydligt ställa krav på den fysiska säkerheten, men när det gäller den digitala säkerheten är det svårare. Dessa båda perspektiv måste ses i ett sammanhang.

Ytterligare en aspekt är personsäkerhet och där måste både de anställdas arbetsmiljö säkras men också i förekommande fall personkontroller göras.

En rekommenderad metod är att till att börja med utreda behovet av säkerhet och sekretess och dokumentera det i en säkerhetsanalys. Analysen ska ge svar på vilka hot som finns, vad som ska skyddas och på vilket sätt. Det finns olika hjälpmedel att tillgå och både Myndigheten för samhällsskydd och beredskap, www.msb.se, och Säkerhetspolisen, www.sakerhetspolisen.se, har tagit fram metoder för att genom en uppsättning administrativa och tekniska säkerhetsåtgärder bevara informationens konfidentialitet, riktighet och tillgänglighet.

Sammanfattning av diskussioner

Det krävs ett ständigt arbete med informationssäkerhet som fastighetsbolag. Det kräver uppföljning av våra olika klassningar med allt vad det innebär. Man måste kontrollera tillgång till olika system, ha rutiner vid exempelvis avslutade anställningar för att de inte ska ligga kvar i systemen.

Förslag på åtgärder:

- Inventera data och genomför informationsklassning.
- Analysera IT-miljön och genomför tester.
- Analysera behörighetsstruktur och olika funktioner/rollers tillgänglighet till information.
- Tidsbestäm tillgänglighet till information (exempelvis under ett projekt)
- Upprätta rutiner för anställningsavslut.
- Ledningens engagemang är central för vägen mot en säker informationshantering.

Avslutningsvis

Våra byggnader blir allt mer smarta och den byggda miljön spelar också en viktig roll i den smarta staden där allt fler funktioner samverkar. Detta ställer krav på bland annat tillgång till data vilket förutsätter att både personer och organisationer är beredda att dela med sig av information. Samtidigt måste vi vara medvetna om säkerhetsaspekten och säkra att inte känslig information sprids och nyttjas felaktigt.

Ett antal av frågeställningarna ovan kräver fortsatt diskussion och kanske fördjupade utredningar och skarpa tester. Genom branschsamverkan kring strategier för digitalisering och utvecklad informationshantering kan utvecklingen påskyndas och förhoppningsvis kan arenan inspirera till fortsatt samarbete och informationsutbyte.

SISAB
Skolfastigheter i Stockholm AB

Här når ni oss:

Pouriya Parsanezhad
pouriya.parsanezhad@sisab.se

Madeleine Lilja
madeleine.lilja@sisab.se

Lars Lidén
lars.liden@metafa.se

Marie Ungheden
marie.ungheden@sisab.se

Rebecca Nyberg
rebecca.nyberg@sisab.se

EN DEL AV STOCKHOLMS STAD

SISAB, Skolfastigheter i Stockholm AB

Postadress: SISAB,
Box 5010,
121 05 Stockholm

Besöksadress:
Palmfeltsvägen 5, v. 5
121 62 Johanneshov

Tel: 08-508 460 00
Fax: 08-508 460 01
Org.nr: 556034-8970

sisab.se
linkedin.com/company/sisab