



FOTO: SÖREN DANIELSSON

Datorstyrt hem genom internet. I Watford, England görs försök att driva ett hem och hushållsutrustning med hjälp av dator. En web-kamera i fönstret i köket bredvid en kaktus och flaskor med vinäger/olja.

Allt mer IT i fastighetsvärlden ger ökade risker och möjligheter

Att utnyttja alla de fördelar som IT ger är ofta inte särskilt svårt eller besvärligt. Det är bara att strunta i konsekvenserna, sticka huvudet i sanden och köra på. För den som vågar höja blicken är det vanligtvis bara är en tidsfråga innan den digitala tsunamin sköljer över företaget och den egna verksamheten. Och precis som vid många naturkatastrofer blir det vanligtvis oerhört dyrt.

AV JOAKIM VON BRAUN, HIGH PERFORMANCE SYSTEMS AB

Det finns ju ingen som kan undgå att se alla tidningsrubriker om digitala hot och risker. Och även om mycket kan vara överdrivet eller röra andra branscher eller sektorer i samhället, så kan ju inte allt vara överdrivna larm från försäljare eller skrämmande historier från myndigheterna. Det finns en verklighet som varje företag måste vara medveten om för att undvika helt onödiga förluster i pengar, tid, renommé och annat.

Det senaste decenniet har inneburit stora förändringar för byggnads- och fastighetsbranscherna. Från att mest ha handlat om ekonomi och allmän administration har IT allt mer kommit att handla om styrning av en rad system som värme och kyla, ventilation, el, inbrotts- och brandlarm och mycket annat både för förvaltning och för hyresgäster. Ungefär samtidigt har det blivit av allt större vikt att kunna erbjuda sina hyresgäster grundläggande IT-funk-

tioner och möjlighet att påverka den interna miljön för personalens trivsel men också av olika ekonomiska skäl.

GÅRDAGENS HOT OCH RISKER

Under många år har de hot och risker som anses som allvarliga antingen utgjorts av datavirus och liknande skadliga program, som sprider sig till samtliga oskyddade datorer, eller hackers vars främsta måltavlor varit företag och myndigheter med en helt

annan profil än svenska bygg- och fastighetsföretag. Eftersom denna hotbild varit gällande från slutet av 1980-talet och en bit in på 2000-talet har många företag invaggats i ett bedrägligt lugn. Bara man hade ett uppdaterat antivirusprogram och tog sina säkerhetskopior kunde man lugnt luta sig tillbaka, ofta också med rätta.

Nu har emellertid IT-världens hot och risker dramatiskt förändrats sedan våren 2003. Och när en mängd variabler förändras ger historien inte alls någon bra bild av hur framtiden ska komma att gestalta sig. Skulle någon till exempel vara beredd att strunta i att teckna en brandförsäkring med hänvisning till argumentet att det aldrig brunnit tidigare?

PENGAR ÄR ALLT

På mindre än tolv månader under 2003–2004 förändrades motiven för hackers, virusskribenter och andra databrottslingar till att helt och hållet handla om pengar. Pengar är uppenbarligen ett mycket mer kraftfullt motiv till att bedriva databrottslighet än alla tidigare motiv tillsammans. Detta har medfört att antalet ekonomiska databrottslingar mångdubblats under en förhållandevis kort tidsperiod, att angreppsmetoder både blev fler och mer avancerade samtidigt som de unga data-

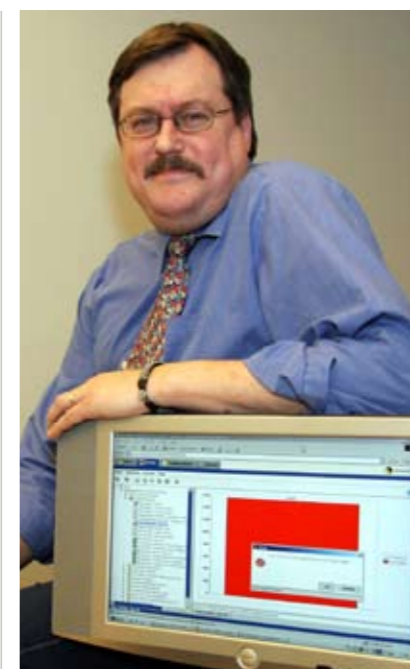


FOTO: JAN-PETER ALM

Joachim von Braun

brottslingarna snabbt fick goda kontakter med andra ekonomiska brottslingar – de som visste hur man skulle förfara för att lura stat och företag på pengar.

Förutom mer traditionell databrottslighet som hacking och virusspredning, har situationen kommit att omfatta kreditkortsbedrägerier, momsbedrägerier,

smuggling, utpressning, skalbolagsaffärer, penningtvätt, piratkopiering, identitetsstöld, försäljning av falska pass och körkort, falska bidrags- och låneansökningar, kontakter för prostitution, narkotikasmuggling och försäljning på internet inklusive andra slags droger och receptbelagda mediciner, intrång på bankkonton, samt en mängd andra brottsmetoder.

DATA HÅLLS SOM GISSLAN

Exempelvis har en helt ny typ av synnerligen elaka trojanska hästar (ett slags datavirus) dykt upp som kallas för »ransomware« (gisslanprogram). De är specialtillverkade för att när de tagit sig in på ett företags server exempelvis kryptera kundregister, ekonomidatabaser, mappar med offerter och liknande. Eftersom de starkt krypterade filerna är försedda med avancerade lösenord blir all denna viktiga interna information plötsligt fullständigt otillgänglig för det drabbade företaget. Och efter en kortare tid erbjuds det drabbade företaget att få köpa lösenord till den krypterade informationen som på så sätt hålls som gisslan till dess man betalar.

En annan variant är att delar av företagets konfidentiella information kopieras av brottslingarna som sedan begär stora pengar för att antingen inte publicera den stulna informationen på internet eller låta bli att sälja informationen till konkurrerande företag. Även om det inte låter så sannolikt att svenska konkurrenter skulle köpa stulen företagsinformation så är risken uppenbar om man jobbar internationellt. För ett par år sedan drabbades Ericsson av att en ungersk hacker vandrade in bland deras serverar och stal ytterst hemlig information från företaget som han senare hotade att publicera ute på internet.

ALLT MER IT I BYGG- OCH FASTIGHETSBRANSCHEN

Från att ha varit en förhållandevis konservativ bransch som endast tagit små, försiktiga steg har fastighetssidan allt mer tvingats in i en allt snabbare digitalisering, både för att bättre kunna förvalta byggande och innehav men också för att kunderna har större behov och ställer allt mer detaljerade krav. Med ett allt kraftigare och smartare utnyttjande av IT finns det nämligen både stora pengar att tjäna samtidigt som man kan skapa fler tjänster att sälja. Tyvärr ▶



FOTO: MARKELKALDERON

En helt ny typ av synnerligen elaka trojanska hästar (ett slags datavirus) har dykt upp som kallas för »ransomware« (gisslanprogram). De är specialtillverkade för att när de tagit sig in på ett företags server exempelvis kryptera kundregister, ekonomidatabaser, mappar med offerter och liknande.

► missar många att det också finns en baksida – en baksida i form av ökad riskexponering och risk för större förluster. Dessa förluster är dock inte endast direkta ekonomiska sådana, det kan exempelvis också röra sig om stora förluster av ett företags goda renommé, vilket kan ta mycket längre tid att reparera än de direkta ekonomiska förlusterna.

ADMINISTRATION

Allt mer av byggande, administration och styrning ligger idag på IT till båtnad både för byggare och förvaltare å ena sidan, och deras kunder å den andra. Det kan röra sig om ritningar som numera finns lagrade på en server, vilket förenklar tillbyggnad och renovering samt kontakter med myndigheter. Med IT går det att låta kunderna

kontrollera till exempel hyra i förhållande till lokalernas yta samt enkelt meddela förändringar till hyresvärderna som att man till exempel flyttat en vägg.

Att system som reglerar värme och kyla, drift-, inbrotts- och brandlarm, tillträde till lokalerna, hissar och rulltrappor, ventilation och mycket annat är digitala och möjliga att nå för personalen via ett Web-interface förenklar och underlättar naturligtvis oerhört mycket. Man kan snabbt och enkelt nå data och olika åtgärder kan snabbt rapporteras. Arbete och leveranser som ska faktureras görs i en handvändning. Mycket kan kollas med hjälp av Web-kameror.

Samtidigt är systemen genom sina Web-interface vanligen enkla att angripa. Det kan både röra sig om okynnesverksamhet och om mer avancerad brottslighet, till exempel utpressning. Och det rör sig nu inte bara om stöld av information. Den kanske största risken är att någon riktar en så kallad Denial of Service-attack mot något av systemen. Det är ingen risk för att information förstörs eller stjäls utan problemet är att attacken gör det helt omöjligt att nå datorn och därmed förhindrar man att drabbade kan skicka instruktioner till systemet via internet. Då måste det till att man har en reservfunktion i form av personal som kan ge sig till platsen och utföra åtgärderna för hand.

VEM ÄR HYRESGÄST?

Det finns främst två omedelbara aspekter på vem man har som kund. För det första rör det sig om en mängd tjänster som kan erbjudas hyresgästen, både sådant som gör lokalerna mer attraktiva och enklare att hyra ut, och sådant som en förvaltare och hyresvärd kan införa för att tjäna pengar på. Det rör sig om ett helt batteri av åtgärder som kan vara attraktiva för kunden och som naturligtvis är mycket enklare och billigare att införa om de finns med redan från början i planeringen när lokaler ska byggas och iordningställas. Dessa åtgärder börjar i ena änden med färdiga kanaler för att kabel enkelt ska kunna dras eller att kabeln redan finns dragen och att många av uttagen redan finns på plats. Den andra änden av möjliga åtgärder finns i hyresvärdens fantasi och är bara beroende på begränsningar av fantasi, idéer och ekonomiska satsningar.

Skillnaden mellan idag och hur det såg ut förr

Virushotet har ökat

2001 upptäcktes 100 nya virus, maskar och trojaner per månad
2008 upptäcks över 10 000 varje månad

2001 uppdaterade man Antivirusprogrammet en gång per vecka
2008 bör man uppdatera det minst en gång per timme

Hackers arbetar för pengar

2001 var hackers nyfikna ungdomar
2008 är de ekonomiska brottslingar

2001 drabbades Pentagon och CIA
2008 drabbas alla som har pengar och persondata

Uppdatera dataprogrammen ofta

2001 hackade man sig in från Internet
2008 hackar sig trojaner från en PC på insidan

2001 skulle man köpa brandväggar
2008 ska man täppa igen egna säkerhetshål genom uppdateringar

Alla är drabbade

2001 drabbades endast ett fåtal företag
2008 kan alla företag råka illa ut

2001 skulle man byta ut Microsoft-program som var sårbara
2008 kan alla program, också egenutvecklade, vara sårbara

IT är inte bara datorer

2001 var IT samma sak som datorer
2008 finns IT överallt

2001 räckte lösenord och antivirus
2008 måste säkerheten skräddarsys efter verksamheten

Elaka datavirus

2001 förstörde virus och maskar ofta information
2008 kryper trojanerna under radarn utan att synas

2001 hjälpte ett uppdaterat Antivirusprogram
2008 måste man också ha personliga brandväggar och uppdatera dataprogrammen regelbundet



FOTO: THORD SKOLDEKRANS

En annan aspekt som ökar i betydelse är bjuda särskilda IT-lösningar för att kunna emot en sådan hyresgäst. Det kan exempelvis vara företag som har en förhöjd hotbild på grund av att de hanterar stora ekonomiska värden såsom banker, aktiemäklare, spelföretag och liknande. En annan kategori kan vara hyresgäster som löper en större risk för attacker av politiska skäl. Det kan röra sig om företag som kommer från vissa länder som Israel, USA eller producerar varor som kan vara kontroversiella – kött, päls och skinn, vapen, tobaksprodukter etcetera. En rad andra liknande risker finns naturligtvis också.

Avslutningsvis är det viktigt att framhålla att precis som att det i första läget är lätt att falla i farstun för alla olika fördelar som de nya IT-tjänsterna kan medföra och då glömma bort att det också finns faror, är det lätt att kastas åt andra hållet och bara

se alla faror och möjliga problem. Ett ordspråk säger att »Man kan göra affärer med en bedragare, bara man vet om att han är just en bedragare«. Slutsatsen är att om man förbereder sig på det som skulle ha kunnat bli en negativ överraskning, så uppstår inte någon överraskning och man kan gå helskinnad genom affären. På samma sätt är det med säkerhetsfrågor. Vet man vilka hot och risker som finns, kan man motverka dem och därmed undvika de obehagliga överraskningarna. Kan ett företag para sina kunskaper om den egna verksamheten och vad som där är skyddsvärt med kunskap om de hot och risker som man därmed kan utsättas för, kan affärsrisken göras helt acceptabel. Precis som inom andra områden i affärsverksamheten kan också IT-området göras säkert och lönsamt. ■



www.projektengagemang.se