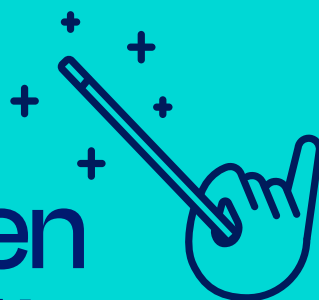


8 steg till en cybersäker retailkedja

(utan att spräcka din it-budget)

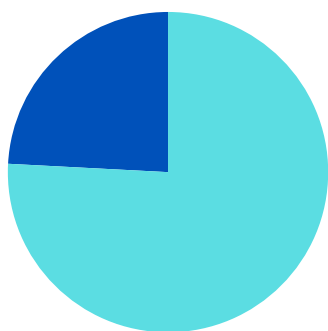


Från gästnätverk i lokalerna till kassasystem i molnet: konnektivitet är affärs-kritiskt inom retail idag. Digitaliseringen medför enorma möjligheter, men även utmaningar i form av en ökande cyberbrottslighet och hårdare konkurrens om eftertraktad it-kompetens. Det tuffa konjunkturläget gör det samtidigt svårt för företagen att avsätta en tillräcklig budget för att möta behoven.

Detta sätter dig som it-chef inom retail i en komplicerad sits. Du behöver möta förväntningar på teknik som "bara ska funka" i en organisation vars kärnverksamhet handlar om helt andra saker. Du måste följa allt hårdare regelverk inom cybersäkerhet. Dessutom behöver du göra detta med begränsade resurser, där du visserligen kan outsourca många delar, men aldrig det grundläggande ansvaret.

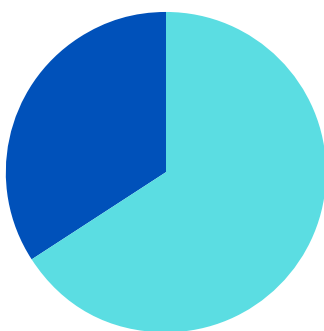
Checklistan här nedanför är tänkt att hjälpa dig hitta en väg framåt för att jobba kostnadseffektivt men ändå säkert, på ett sätt som är långsiktigt hållbart. Vi hoppas du har användning för råden.

Hur ser dilemmat ut i siffror?



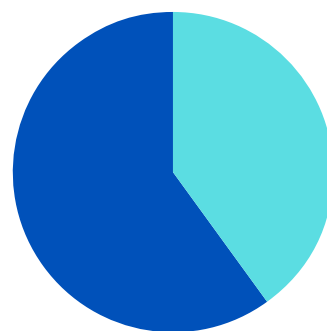
76%

av it-cheferna oroar sig för cyberattacker eller it-haverier.



66%

är beroende av specifika individer för att drifva företagets nätverkslösning.



40%

anser att it-budgeten är för liten i relation till verksamhetens förväntningar.

8 punkter för cybersäkerhet som lönar sig i längden

1. Sätt en end-to-end-strategi för säkerhet (och förankra den i organisationen)

Ledordet för ditt cybersäkerhetsarbete bör vara “end-to-end”. Det innebär att säkerheten byggs in i varje led av företagets it-infrastruktur – istället för att slängas på i efterhand som något “extra”. Hela organisationen måste inse hur affärskritisk frågan är. Samtidigt behöver du förstås hushålla med de resurser som finns. En tydlig och väl förankrad strategi hjälper dig både att argumentera för din it-budget och använda den effektivt.

5 nyckelfrågor att besvara när du utformar din strategi är:



- Vilka krav har ni på nätverkens hastighet och tillgänglighet?
- Vilka enheter måste vara uppkopplade mot nätet?
- Vilka avdelningar och användare ska ha åtkomst till vad?
- Vilka servrar, portar och ip-adresser behöver kunna kommunicera med varandra?
- Vilka krav ska ni ställa på support från era leverantörer – behöver ni kunna be om hjälp dygnet runt, eller räcker det med vanliga kontorstider?

2. Segmentera nätverken för att minska skadan vid intrång

När du har kartlagt behoven av uppkoppling och åtkomster måste du säkerställa att din strategi implementeras och upprätthålls ända ut i varje butik, kafé eller lager. Dagens cyberbrottslingar tar sig nämligen sällan in via uppkopplade enheter på ett företags huvudkontor. Istället utnyttjar de säkerhetsluckor längre ut i organisationsstrukturen, för att därifrån ta sig uppåt i hierarkin tills de når en behörighetsnivå där de kan stjäla känslig data eller slå ut affärskritiska funktioner. Genom att segmentera dina nätverk hindrar du angriparna från att ta sig vidare efter ett initialt intrång, vilket effektivt begränsar skadan de kan ställa till med.

3. Kontrollera trafikflödena med SD-WAN

I takt med att fler verksamhetskritiska funktioner flyttas till molnet växer behoven av säkra och flexibla nätverkslösningar. Med den mjukvarubaserade tjänsten SD-WAN (Software-Defined Wide Area Network) kan du övervaka, prioritera och kryptera trafikflöden mellan uppkopplade enheter – inklusive molntjänster. Genom att sätta upp regler centralt för hur olika flöden ska hanteras skyddar du känsliga uppgifter och hindrar skadliga intrång från att spridas. Dessutom kan du fördela dataprestandan dit den för tillfället behövs, istället för att hålla igång tjänster och processer i onödan. Därmed använder du dina resurser på ett effektivare sätt.

4. Satsa på en ordentlig brandvägg

En brandvägg är en hygienfaktor för dagens företag. Men för att ge ett effektivt skydd behöver brandväggen:



- Kunna konfigureras för att blockera respektive släppa igenom rätt trafik
- Optimeras prestandamässigt för stabilt skydd även vid stora mängder data
- Vara skalbar så att skyddet kan anpassas efter växlande behov
- Uppdateras kontinuerligt för att skydda mot de senaste hoten och intrången

Att löpande konfigurera, optimera och övervaka din brandvägg kräver mycket tid och resurser internt. För att minska individberoendet som detta innebär, och därmed sårbarheten för organisationen, väljer många företag att outsourca sin brandvägg och köpa den som managerad tjänst (managed firewall). Det ger ett garanterat uppdaterat skydd till en förutsägbar kostnad.

5. Välj utrustning med kvalitet

Med en pressad budget är det lockande att kapa kostnader överallt där det går. Men när du snålar med kvaliteten på hårdvaran riskerar du att få potentiellt kostsamma säkerhetsluckor på köpet. Billigare utrustning tenderar också att ha kortare livslängd och behöver därför bytas ut oftare, vilket kostar material och arbetstimmar.

En brandvägg är
en hygienfaktor för
dagens företag.



6. Framtidssäkra för compliance – och konkurrenskraft

Kraven på cybersäkerhet och hållbarhet ökar från såväl konsumenter som lagstiftare. Företag i allt fler sektorer och led i leveranskedjan måste kunna visa hur de tar ansvar för saker som:

- Energianvändning och materialåtervinning hos hårdvaruleverantörer
- Klimatpåverkan från datacenter som företaget använder
- Rutiner och åtgärder vid cyberangrepp

Det du investerar i hållbara lösningar idag kan du alltså räkna hem i framtiden i form av större förtroende från kunder, mindre risk för kostsamma cyberangrepp – och genom att undvika omfattande böter för bristande regelefterlevnad. I längden lönar det sig därför att välja it-leverantörer som både arbetar aktivt med hållbarhet och uppfyller relevanta ISO-certifieringar inom datasäkerhet.

7. Jobba skalbart och flexibelt – utan att kompromissa med säkerheten

I ekonomiskt osäkra tider är det svårt att ta beslut om långsiktiga investeringar som exempelvis nya lokaler. Tillfälliga popups har blivit ett populärt sätt för fysiska butiks- och restaurangkedjor att bli mer agila i var de möter sina kunder. Men när en ny location ska etableras på kort tid riskerar cybersäkerheten att bli lidande. Även här är den mjukvarubaserade nätverkslösningen SD-WAN ett smart alternativ. Du får direkt en säker och stabil uppkoppling med krypterad trafik och kan enkelt lägga till eller ta bort platser utifrån behov.

8. Etablera ett tydligt SLA för trygghet, tydlighet och minskad administration

En viktig del av drift- och cybersäkerhetsarbetet är att tydliggöra vilka garantier som ingår i avtalen med dina it-leverantörer. Se därför till att alltid ha ett tydligt SLA (Service Level Agreement) som är anpassat efter just din verksamhets behov, till exempel när det gäller förväntad svarstid på felanmälningar. Du vill inte betala för en högre servicenivå än du behöver, men inte heller riskera att vänta onödigt länge på hjälp i fall där varje minuts nertid innebär förlorade intäkter.

Ofta lönar det sig att samla flera tjänster hos en och samma partner. För ju mindre tid och resurser du och dina medarbetare behöver lägga på att till exempel:

- administrera avtal med olika it-leverantörer
- felsöka krånglande nätverk
- byta ut trasig eller utdaterad utrustning

...desto mer kan ni fokusera på att driva verksamheten framåt och uppnå era affärsmål.

Om GlobalConnect

Vi på GlobalConnect är den ledande leverantören av fiberbaserad datakommunikation och datacenter i norra Europa. Med 155 000 kilometer egen fiber i marken kopplar vi upp och ihop Sverige och våra 30 000 företagskunder med resten av världen. Det kan handla om att koppla ihop butiker som ingår i en kedja, att förse små och medelstora företag med säker uppkoppling till att bygga datacenter åt några av världens största och mest krävande kunder. Vi sysslar även med nätverk, kommunikation och infrastruktur. Kort sagt gör vi det mesta inom uppkoppling.

Vi har lång erfarenhet av att ta fram skräddarsydda lösningar för retail. Bland våra kunder finns kedjor som Stadium, Clas Ohlson, Systembolaget och Lyko. Läs gärna om våra tjänster för detaljhandeln på vår [hemsida](#) eller [kontakta oss direkt](#) om du vill veta mer.