Digitaliseringen ställer nya krav på säkerhet

Microsoft

Digitaliseringen är här för att stanna

Digitaliseringen öppnar nya möjligheter för företag, men med digitaliseringen kommer också nya typer av säkerhetshot som företag behöver förhålla sig till. Cybersäkerhet är ett område som växer i takt med att hoten ökar. När vi blir mer mobila och använder teknik i en större utsträckning, hur säkerställer man då säkerheten och undviker de risker och hot som finns? Säkerhetshot är vanligare än vad man tror, och medianvärdet av antal dagar som det tar för företag att upptäcka intrång är 200 dagar. Det leder inte bara till frågan om hur företag kan skydda sig, men också hur man kan upptäcka och hantera intrång.

Med modern teknik följer en säkerhet och ett skydd anpassat efter hur vi jobbar i dag och de hot vi utsätts för nu och i framtiden - oavsett om det handlar om virus via mejl eller att slippa oroa sig för att information ska komma i orätta händer om en mobil stjäls eller hamnar på villovägar.

Nya krav på organisationer

I dag spenderar anställda 50 procent mer tid på att samarbeta med andra och 37 procent av den globala arbetskraften är mobil. Att låta medarbetarna nå affärssystem och jobbmejl hemifrån är förstås positivt för verksamheten, och nya digitala verktyg för samarbete ger medarbetarna en möjlighet att vara mer produktiva. Men detta medför även en ökad sårbarhet för intrång och läckor.

Dagens IT-brottslingar är välorganiserade och ytterst professionella. De har tillgång till avancerade verktyg och är ute efter att tjäna pengar där det är möjligt. Hela 43 procent av alla cyberattacker riktar sig mot små företag – även företag som inte ser sig själva som särskilt intressanta mål riskerar att drabbas av intrång. Ett intrång kan innebära att företaget blir av med affärskritisk information, eller får sin data krypterad för att sedan behöva betala en lösensumma för att få den tillbaka. Utvecklingen har gått enormt fort, och många företag har ännu inte hunnit anpassa sin säkerhet till den nya verkligheten.

I detta whitepaper kommer vi att se närmare på de risker och krav som företag ställs inför i takt med att verksamheten blir mer digitaliserad.

Microsoft

Nya hotbilder

De senaste åren har IT-säkerhet placerats allt högre på agendan hos företag. Anledningen är att cyberhoten både ökar och blir mer sofistikerade.

Enligt Försvarets radioanstalt (FRA) sker tiotusentals attacker mot svenska mål varje månad. I sin årsrapport 2016 konstaterar myndigheten att säkerheten på många håll inte är dimensionerad för den hotbild de ser, samt att det ”med relativt enkla metoder och med kända angreppsverktyg går att ta över nätverken utan större problem”. Det bör nämnas att FRA i sina säkerhetsgranskningar riktat in sig på myndigheter och statliga bolag, men poängterar att hotbilden omfattar alla, till och med privatpersoner som saknar koppling till skyddsvärd verksamhet kan bli föremål för angrepp. Det kan exempelvis ske genom att deras datorer används för att skapa ett nätverk av datorer som angriper ett mål någon helt annanstans.”

FRA är känt för sin operationssekretess. Att myndigheten offentliggör så här mycket information är därför en tydlig signal om att man ser allvarligt på läget.

Vanliga säkerhetsbrister hos organisationer, enligt FRA:

- Otillräcklig kunskap om hotbilden
- Bristande förståelse hos ledningen för behov av åtgärder
- Outsourcing skapar sårbarheter
- Bristande kravställning vid nya upphandlingar och avtal

Yttre hot

Dagens cyberangripare, oavsett om det är kriminella, ”hacktivister” eller statliga aktörer, är professionella och har resurser att utföra mycket sofistikerade attacker. Till sitt förfogande har de avancerade uppsättningar verktyg och tekniker som ofta lämnar ytterst få spår och kan orsaka stor skada, beroende på syfte. Det råder fortfarande stor okunskap i samhället om hur omfattande dessa attacker är, då drabbade företag sällan vill berätta offentligt att de hackats och majoriteten av fallen når aldrig media. Sätten på vilket ditt företag kan drabbas är många. Det kan ske både med och utan skadlig kod som virus eller ransomware, och det innebär att antivirusprogram inte är ett tillräckligt skydd.

Opportunistiska hackers är ute efter att lyfta ur maximala mängder information så snabbt som möjligt efter ett lyckat intrång. Lösenord och intressanta filer kopieras, ofta till en dator på andra sidan jorden, vilket försvårar det juridiska efterspelet till hackerns fördel. När intrånget inte upptäcks kan hackern etablera en långvarig närvaro i nätverket (det finns exempel på inkräktare som härjade ostört i flera år innan upptäckt), och under lång tid samla in information som senare kan användas till exempel i ett avancerat bedrägeri.

Hackad e-handel blir allt vanligare, eftersom branschen växer i raketfart. Det vanligaste huvudmålet är detaljhandeln, och en studie (Trustwave 2015) visar att 64 procent av alla brott mot detaljhandeln det året berodde på brister i e-handelsmiljön. E-handelsplatser är enormt lukrativa, eftersom de dels hanterar dina kunders pengar, dels kan generera olika typer av kunddata som lösenord och kreditkortsuppgifter.

ID-kapning är också ett växande problem: varje dag beräknas cirka 350 personer få sin identitet kapad. IT-säkerhetsföretaget F-Secure rapporterar att en vanligt förekommande metod är att bedragaren utger sig för att vara vd eller annan högt uppsatt chef, och skickar ett mejl till ekonomiavdelningen med instruktioner om att betala en falsk faktura. Även mer sofistikerade metoder, som banktrojaner, förekommer.

Malware är samlingsnamnet på olika former av skadlig programvara, där virus och trojaner är de mest kända. På senare tid har **ransomware** blivit populärt. Utpressningen går ut på att programmet krypterar datorns innehåll så att filerna blir oläsliga såvida inte den drabbade betalar en summa pengar för ett lösenord som återställer innehållet.

Inre hot

Intrång behöver inte alltid komma utifrån. Några av de allvarligaste hoten mot ditt företags IT-integritet kommer ofta inifrån – det kan vara så enkelt som att en av dina anställda laddar ner en app som innehåller skadlig kod.

Den mänskliga faktorn – alla kan göra misstag och några exempel på sådant en medarbetare kan göra utan att inse hur det kan påverka företaget är att använda privata mejl- eller lagringstjänster för företagsinformation, inte använda sig av lås på telefon och datorer i offentliga miljöer, glömma telefonen på bussen, eller att prata om inloggningsuppgifter och rutiner i fel sammanhang och med fel personer.

Obehörig åtkomst är kanske allvarligast i branscher som hanterar känsliga uppgifter, men alla företag har information som kan orsaka företaget åtminstone viss ekonomisk skada om den läcker ut. Här finns allt från personal i hälsovårdssektorn som obehörigt läser patientjournaler till illojala medarbetare som exempelvis vid en uppsägning bestämmer sig för att sabotera eller stjäla företagshemligheter. Även lojala och ärliga medarbetare kan utgöra en risk, ifall deras användarkonton vid ett intrång visar sig ha alltför långtgående behörigheter i IT-miljön.

Även rent **illegal aktivitet** kan bli ett problem. I USA och Storbritannien finns exempel på anställda som orsakat arbetsgivaren utredningar och i vissa fall böter efter att ha använt företagets IT-system för att ladda ned och distribuera upphovsrättsskyddat material.

Social manipulation är en av de vanligaste metoderna för åtkomst till ett företagsnätverk. Fler än en medarbetare stoppar gladeligen in ett usb-minne de hittat i receptionen i sin dator, utan att misstänka att det kan vara preparerat med spionprogram. Att råka avslöja känslig information över telefon till en bedragare är inte heller ovanligt. Så kallad social manipulation är av de svåraste angreppsmetoderna att skydda sig mot.

Microsoft

Molnet – ett säkrare alternativ

Leverantörer av molntjänster har i de flesta fall långt mer kunskap och resurser att sätta upp och driva säkra IT-miljöer, än vad många företag själva har. Lokala servrar erbjuder visserligen ökad kontroll över hårdvaran, men många företag saknar spetskompetensen som idag krävs för att skapa och upprätthålla ett system med tillfredsställande säkerhetsnivå.

Molnleverantörer har också långt bättre möjligheter att sätta in motmedel vid en attack. De betjänar hundratals eller tusentals kunder, och övervakar hotbilden dygnet runt. Vid behov kan en uppdatering sjösättas eller ett säkerhetshål täppas till omedelbart hos samtliga användare, helt utan din inblandning. Och medan molnleverantören ser till att alla certifikat och virussignaturer hålls uppdaterade, dygnet runt, kan du fokusera på din kärnverksamhet.

Molnets skalbara och decentraliserade arkitektur gör det mer motståndskraftigt mot såväl överbelastningsattacker som naturkatastrofer, inbrott och strömavbrott.

Även de ekonomiska aspekterna bör vägas in, speciellt för mindre företag kan molnet erbjuda ett prisvärt alternativ till en lokal IT-miljö, med en säkerhetsnivå få mindre företag skulle ha råd att upprätthålla.

IT-säkerhet och GDPR

Den 25 maj 2018 börjar den nya dataskyddsförordningen att gälla i EU:s medlemsländer. The General Data Protection Regulation (GDPR) ersätter i Sverige den nu gällande personuppgiftslagen (PUL) och innebär på flera sätt en skärpning av regelverket kring hantering av personuppgifter. Nuvarande dataskyddslagstiftning bygger på ett EU-direktiv från 1995 – när faxmodem var moderna och smartphones ännu inte uppfunna – och får anses vara föråldrad på flera områden, något som GDPR är tänkt att åtgärda.

Syftet med GDPR är att ge privatpersoner ökat inflytande över sina personuppgifter och bättre kontroll över hur dessa får hanteras och lagras av företag och myndigheter. Förordningen kommer därför att gälla samtliga företag och organisationer som sparar eller på något sätt hanterar personuppgifter, oavsett storlek. Personuppgifter kan förekomma i en mängd olika former, som alla omfattas: anställningsavtal, kundregister, lönedatabaser för de anställda eller textdokument med anteckningar inför ett event om vilka kunder som är allergiska mot skaldjur.

Ur ett IT-säkerhetsperspektiv påverkar GDPR framförallt två områden: dataskydd och rapportering vid dataintrång:

Inte bara utmaningar

Det är lätt att glömma att GDPR innebär många fördelar. Daniel Akenine, säkerhetschef på Microsoft Sverige, listar fem av dem:

- Ger människor bättre kontroll på vilka data som sparas och var.
- Modern lagstiftning som passar det digitala samhället bättre.
- Nytt juridiskt ramverk som gör det lättare för företag att verka inom EU.
- Rapporteringsskyldighet vid intrång skapar mer kunskap om problemen.
- Ökad transparens gör det lättare att fatta beslut om vilka företag man kan lita på.

Dataskydd

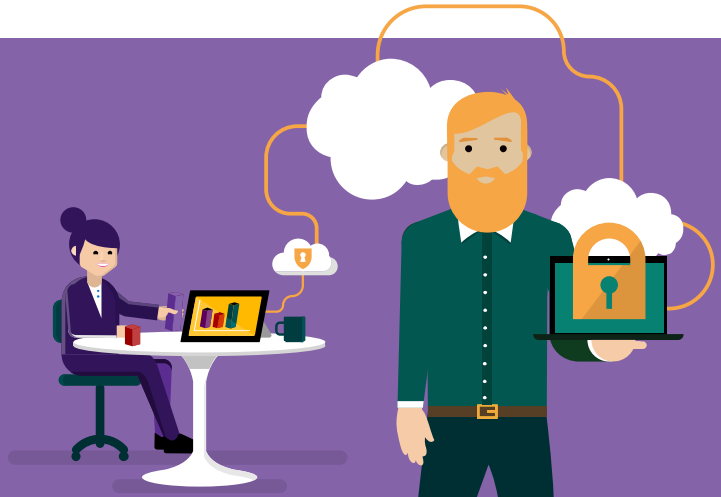
En av de centrala punkterna i GDPR är ”privacy by design” – på svenska ”inbyggt dataskydd” eller ”dataskydd som standard”. Kravet innebär att företag implementerar såväl tekniska som organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas. Detta är ett omfattande krav med långtgående tekniska konsekvenser, som kan sammanfattas i att datasystemen ska vara utformade på ett sådant sätt att personuppgifter inte samlas in eller behandlas i onödan, och ”pseudonymiseras” så tidigt det går. Pseudonymisering är en form av reversibel anonymisering, och innebär att personuppgifterna bearbetas på ett sådant sätt att de blir omöjliga att knyta till en specifik person utan ytterligare information – vilket ökar skyddet vid en eventuell personuppgiftsincident.

Personuppgiftsincidenter

Så kallade ”personuppgiftsincidenter” ska enligt GDPR rapporteras till ansvarig myndighet, i Sverige Datainspektionen (DI), inom 72 timmar efter att de upptäckts, om det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. En incident kan till exempel vara ett borttappat usb-minne med personuppgifter, en stulen laptop, ett dataintrång på en av företagets servrar eller en anställd som obehörigt tagit del av personuppgifter. Anmälan måste bland annat innehålla information om viken typ av uppgifter som berörs, en beskrivning av troliga konsekvenser av incidenten samt en beskrivning av vilka åtgärder som företaget planerar att vidta för att minimera skadan av det inträffade.

GDPR ställer hårda krav på företagen. Det företag som bryter mot reglerna riskerar böter på upp till 20 miljoner euro, eller 4 procent av företagets globala omsättning. Införandet av GDPR kommer i många organisationer innebära att nya rutiner behöver införas för att hantera register på ett säkert sätt, och kommer också att ställa nya krav på ledningen.

En modern IT-miljö med effektiva säkerhetssystem kan skydda ditt företag mot såväl avsiktliga som oavsiktliga dataintrång, och på så sätt underlätta för er att uppnå kraven i GDPR.



Microsoft

Så skyddar du ditt företag

Modern hårdvara

Modern hårdvara kommer med inbyggd teknik som underlättar att hålla en säkerhetsnivå som äldre enheter ofta har svårt att leva upp till. Detta gäller allt i från säker inloggning med biometri till datakryptering med Trusted Platform Module (TPM) chip och uppkoppling till trådlösa nätverk.

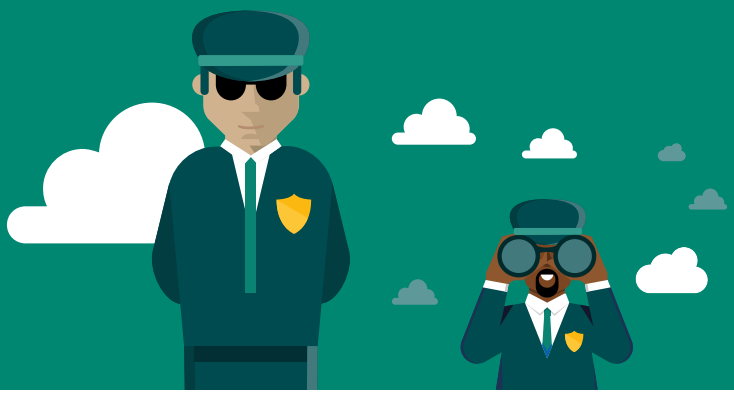
Säkert operativsystem och mjukvara

Mjukvara som inte bara skyddar ditt företag mot intrång, utan även hjälper till att upptäcka och svara på avancerade, riktade attacker låter din organisation fokusera på verksamheten utan störningsmoment. På en telefon som är glömd på bussen kan data enkelt raderas.

Cybersäkerhet bidrar både till en säkrare IT-miljö och underlättar GDPR-efterlevnaden.

Se till att anställda inte kan skicka företagsinformation via sin privata mejladress. Det ska vara svårt för medarbetarna att göra fel. Glöm inte bort att användaren ofta är den svagaste länken i säkerhetskedjan. Det spelar ingen roll hur många brandväggar du satt upp eller hur svåra lösenorden är om en användare frivilligt eller av misstag delar med sig av information.

Microsoft



Summering

Företag angrips utifrån av organisationer och hackare som kan ha såväl ekonomiska som ideologiska motiv. Från insidan kan en illojal eller omedvetet vårdslös medarbetare orsaka allvarligt informationsläckage.

Dagens verklighet är att cyberhoten fortsätter att öka, och hotbilden växer även för mindre företag. Det räcker inte längre att sätta upp ens en ”säker lösning” och hoppas på det bästa – säkerhetsarbetet måste vara en pågående process som genomsyrar verksamheten på alla plan.

I och med GDPR måste även mindre företag se med nya ögon på IT-säkerheten, men genom att implementera en modern molnlösning kan även de minsta företagen få tillgång till branschledande säkerhetslösningar utan att behöva bekosta en stor IT-avdelning.

Säkerheten kommer även fortsättningsvis att behöva vara en prioriterad fråga på företaget, och en pålitlig molnleverantör kan vara en värdefull partner i kampen mot cyberhoten.

Källor

Dataskyddsförordningen (GDPR)

FRA Årsrapport 2016

Myndigheten för samhällsskydd och beredskap:
Informationssäkerhet - trender 2015

Symantec ISTR Financial Threats Review 2017

Symantec ISTR Special Report: Ransomware and Businesses 2016

2015 Trustwave Global Security Report

Akenine, Daniel: Välkommen GDPR!

Nilsson, Tomas: Cyberhoten ökar i finansvärlden

F-Secure Business Security Insider:
ID-kapning är en växande plåga

Harvard Business Review, January-February Issue 2016:
Collaborative Overload

Strategic Analytics:
Global Mobile Workforce Forecast, 2015-2020, November 2015

Small Business Trends:
CYBER SECURITY STATISTICS – Numbers Small Businesses Need to Know, Jan. 3, 2017

Microsoft

Microsoft