Skydda din IT-miljö

En guide till medvetet säkerhetsarbete i mindre teknikföretag

Teknikföretagen

Cyberattacker
mot Sverige per år:
>100 000 st

Antal anmälda
kortbedrägerier på internet
i Sverige per månad:
10 000 st

Antal
allvarliga IT-incidenter
i Sverige per år:
50 st

Antal datorer
i Sverige med virus
eller skadliga program:
17 000 st

Totalkostnad
per år för cyberattacker
mot svenska företag:
16 miljarder kr

Andel företag
i Sverige som saknar
kompetens och resurser
för att klara
cybersäkerhetshot:
50 procent

Antal mobila enheter
i Sverige med virus
eller skadliga program:
400 000 st

KÄLLA: FRA, CERT-SE, NBC-POLISEN, MCAFFE, PTS OCH NTT SECURITY

Skydda din IT-miljö – allt viktigare

Whaling, Phishing, Malware, Cyberattacker …

Det finns en mängd begrepp som beskriver olika typer av dataintrång och identitetsstölder i vår IT-miljö. Företag och individer blir allt oftare utsatta för attacker och behovet av ett medvetet säkerhetsarbete blir allt viktigare. Dataintrång och ID-kapningar drabbar också mindre företag i ökad utsträckning.

Teknikföretagen har över 4 100 medlemmar, varav 3 200 är företag med färre än 50 anställda. För att stötta våra mindre medlemsföretag i arbetet med IT-säkerhet har vi tagit fram denna guide *Skydda din IT-miljö*. Det handlar om att få fördjupad insikt, öka kontrollen, minska riskerna och att minimera skadorna om något händer. Vår förhoppning är att guiden ska bidra till en ökad förståelse för riskerna i informationssamhället och ett mer genomtänkt säkerhetsarbete.

PATRIK SANDGREN
Expert digitalisering, Teknikföretagen

MARIA ROSENDAHL
Enhetschef, Kompetensförsörjning och Digitalisering, Teknikföretagen

Checklista

För ett litet företag kan det vara svårt att veta var man ska börja och vilka områden säkerhetsarbetet bör omfatta. I checklistan har vi samlat de aktiviteter vi rekommenderar att företaget arbetar med. För att få med ett brett perspektiv har vi valt att dela upp aktiviteterna utifrån företaget, företaget och den anställda samt den anställda.

FÖRETAGET

- [ ] Installera och ha uppdaterade virusskydd och brandväggar.
- [ ] Identifiera vilken information som är mest kritisk och vilka som har tillgång till den.
- [ ] Använd en tvåfaktorsautentisering för viktiga konton.
- [ ] Ha kontroll över var ni lagrar er företagsdata och ta backup regelbundet.
- [ ] Kontrollera var er hemsida är placerad, hur eventuella molntjänster hanteras, leverantörens ansvar och om den lyder under svensk lag.
- [ ] Ta fram genomtänkta riktlinjer för säkerhetsarbete.
- [ ] Överväg att förbättra säkerheten med ett VPN (virtuellt privat nätverk).
- [ ] Gör en bedömning av om ert företag kan anses ha högre risk än generellt.
- [ ] Identifiera era vägar ut från företagets system (kunder, leverantörer, maskiner, partners med flera).
- [ ] Stöldmärk utrustning.
- [ ] Ta fram rutiner för hur ni ska agera om ni blir utsatta.
- [ ] Utse någon som är ansvarig för IT-säkerhet på företaget.
- [ ] Anmäl till polisen om ni blir utsatta.

I checklistan har vi samlat de aktiviteter vi rekommenderar att företaget arbetar med.

FÖRETAGET OCH DEN ANSTÄLLDA

- [ ] Sätt riktlinjer för hur lösenord hanteras, det vill säga att starka lösenord väljs och byts ut regelbundet.
- [ ] Ha kontroll över vilka program, applikationer och mjukvara som laddas ner till olika terminaler.
- [ ] Håll programvaror, routrar och operativsystem uppdaterade.
- [ ] Kontrollera att varje anställd uppdaterar virusskydd och brandväggar.
- [ ] Identifiera vilken information som den anställda behöver göra backup på regelbundet.
- [ ] Fundera på vem som har behörighet till vilken information, inför om möjligt behörighetskontroll.
- [ ] Säkerställ att företags- och privatrelaterade konton samt utrustning hålls separerade.
- [ ] Påminn regelbundet om riskerna, gå igenom riktlinjerna och hur de anställda ska agera.

DEN ANSTÄLLDA

- [ ] Följ företagets riktlinjer för IT-säkerhet.
- [ ] Reflektera över vilken infrastruktur som används i olika situationer, var försiktig med att använda publika och oskyddade nätverk.
- [ ] Var misstänksam mot epost från okända avsändare och när bifogade länkar samt filer kommer oväntat.
- [ ] Stäng av bluetooth och internetdelningen när de inte används.
- [ ] Håll programvaror, routrar och operativsystem uppdaterade.
- [ ] Använd lösenord för all utrustning.
- [ ] Håll koll på hur känslig information lagras och kryptera känslig information.
- [ ] Var försiktig med vilka externa tillbehör du ansluter till din utrustning.
- [ ] Se till att utrustning, programvara, routrar, virusskydd, brandväggar och appar är uppdaterade med den senaste versionen.
- [ ] Reflektera över beteendet på sociala medier, hantering av vänförfrågningar, deltagande i särskilda grupper etcetera.

Skydda din IT-miljö

Skydda din IT-miljö är ett stöd för det mindre företaget i ert IT-säkerhetsarbete. Guiden visar på de vanligaste hoten i IT-miljön och vad ni kan göra för att skydda er bättre.

Det digitala inslaget i företagens verksamhet blir allt större och finns med i allt från produktionsprocesser, maskiner, fordon, interaktionen med kunder, leverantörer, partners och myndigheter till administration och ekonomi. Olika system kopplas samman på sätt som vi inte alltid tänker på och som är svåra att överblicka.

Digitalisering genomsyrar allt vi gör och konsekvenserna av om det fallerar växer. Vårt beroende ökar, vi blir mer sårbara vilket tråkigt nog också betyder att vi blir mer utsatta för intrång och cyberattacker. Att drabbas av virus, identitetskapningar eller andra former av angrepp kan bli dyrt och drabba ett företag hårt. Det är svårt att skydda sig, i stort sett omöjligt att skydda sig helt, men det går att vara mer förberedd. Tekniska verktyg behövs men den enskilt största osäkerhetsfaktorn finns i hur varje människa beter sig och använder digitala produkter och tjänster. Genom att höja medvetenheten om de vanligaste riskerna och hur de kan motverkas kan vi också ändra vårt beteende.

Företag, särskilt inom industrin, använder alltmer digitala verktyg i sina tillverkningsprocesser. Att andra enheter än mobiler och datorer också är uppkopplade till internet glöms ofta bort.

För att skydda IT-miljön på lämpligt sätt behöver man förstå vad man kan råka ut för. Vanliga incidenter är:

- Skadlig programvara som placeras i datorer och till exempel förstör information eller kopierar inloggningsuppgifter, det kallas också för malware.
- Ransomware kallas en programvara som låser terminaler, program eller krypterar filer för att därefter kräva ägaren på en lösensumma.
- Företags-, person- och kontouppgifter som sprids till fel mottagare genom till exempel phishing/nätfiske, det vill säga att via e-post luras till att klicka på en länk och ange känslig information, till exempel personliga koder.
- Programvaror och utrustning som inte har uppdaterats och gör företagskänslig information tillgänglig.

Attacker utförs ofta organiserat, det har blivit en egen industri som är ute efter pengar eller för att stjäla information.

De fem viktigaste åtgärderna

Det första steget mot säkrare IT-miljö är att börja arbetet. Ni kan välja att göra det på egen hand eller ta hjälp. Oavsett rekommenderar vi att ni börjar med att:

1. Installera/uppdatera virusskydd och brandväggar
2. Kontrollera att er utrustning kopplas upp på ett säkert sätt
3. Lösenordsskydda, med starka lösenord, utrustning och information
4. Ta fram riktlinjer för företaget och personalen
5. Identifiera företagskritisk information, var den lagras och att ni gör regelbunden backup

Regeringen har beslutat att upprätta ett nationellt center för att öka informations- och cybersäkerheten. Det visar att cyberattacker är ett allvarligt hot i samhället.

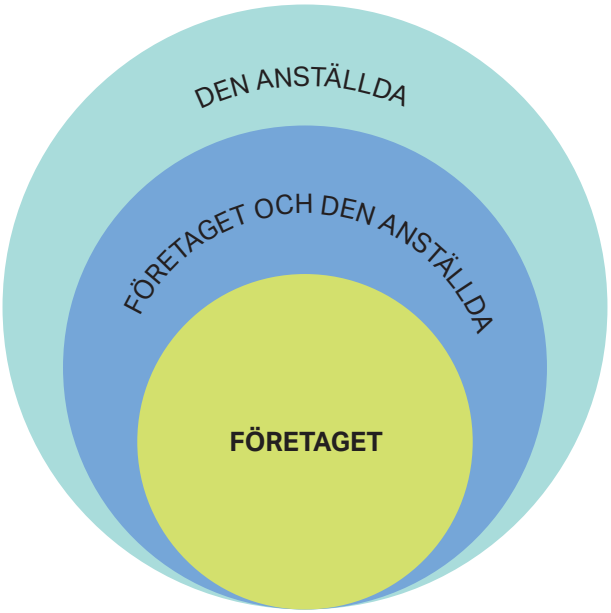

75%
100%
25%
50%
caps lock
shift

IT-säkerhet har olika perspektiv

IT-miljön är mer komplicerad idag än tidigare. Från stationära datorer sammankopplade i ett internt system med lokalt nätverk har vi nu system, program och filer i molnet och vi loggar in på olika typer av nätverk från olika platser. Företagets kontroll över vad som händer och vilka risker som finns blir en allt större utmaning att hantera.

Ett företag behöver betrakta sin IT-miljö ur ett bredare perspektiv än tidigare. Det kan omfatta företagsunika system och nätverk som företaget själv har kontroll över men vanligare är att IT-miljön kontrolleras av någon annan aktör. Det är viktigt att ni reflekterar över var systemen finns, vilka leverantörer som anlitas och hur informationen nås.

Det är också viktigt att reflektera över vem på företaget som använder vilka tjänster, när, till vad och hur det går till. Ett företagsinternt perspektiv behöver ta med personalens situation, både på och utanför arbetsplatsen.



Företaget

Företaget behöver betrakta IT-miljön ur flera perspektiv. Det finns ett tekniskt och ett organisatoriskt perspektiv och det finns ett internt och externt perspektiv. Företag har relationer till personalen, kunder, leverantörer och partners.

Företaget vill att IT-miljön ska fungera så smidigt som möjligt. Det kan göra att lösningar och rutiner som höjer säkerheten kan få för litet utrymme till förmån för enkelhet och effektivitet. Tyvärr kan det leda till kostsamma konsekvenser. Många mindre företag har små resurser och kompetens men också begränsat med tid. Det kan leda till för lite arbete med IT-säkerhet, samt att det saknas genomtänkta rutiner både för att förhindra attacker och för hur företaget ska agera om det blir utsatt. Det blir allt vanligare med virusattacker eller kapningar där information går förlorad, det beror i sin tur på att företaget:

- Inte har uppdaterade virusskydd och brandväggar
- Saknar backup av viktig information
- Inte har kontroll över sitt system i relation till andra
- Inte har gjort en bedömning av säkerhetsriskerna och tagit fram genomtänkta riktlinjer för sitt säkerhetsarbete

Företaget behöver ta ett samlat grepp om sin IT-miljö och sitt säkerhetsarbete. Det finns mycket som kan göras på en övergripande nivå.

- Installera och ha uppdaterade virusskydd och brandväggar
- Identifiera vilken information som är mest kritisk och vilka som har tillgång till den
- Använd en tvåfaktorsautentisering för viktiga konton
- Ha kontroll över var ni lagrar er företagsdata och ta backup regelbundet
- Kontrollera var er hemsida är placerad, hur eventuella molntjänster hanteras, leverantörens ansvar och om den lyder under svensk lag
- Ta fram genomtänkta riktlinjer för säkerhetsarbete
- Överväg att förbättra säkerheten med ett VPN (virtuellt privat nätverk)
- Gör en bedömning av om ert företag kan anses ha högre risk än generellt
- Identifiera era vägar ut från företagets system (kunder, leverantörer, maskiner, partners med flera)
- Stöldmärk utrustning
- Ta fram rutiner för hur ni ska agera om ni blir utsatta
- Utse någon som är ansvarig för IT-säkerhet på företaget
- Anmäl till polisen om ni blir utsatta

Företaget och den anställda

I mindre företag är det vanligt att varje individ får skapa en digital miljö som passar den bäst. Det är viktigt att individen får de verktyg som den behöver för att utföra sina arbetsuppgifter på det sätt som passar denna bäst. Men detta försvårar kontroll av IT-skyddet.

Särskilt små företag lämnar ofta ett större utrymme för sin personal att skapa en IT-miljö som passar var och en. Det är effektivt men gör också att företagets kontroll blir sämre. Den som är ansvarig har kanske inte längre kontroll över vilka program och system som används, hur den anställde väljer att skydda sin information och varifrån. Risker som kan uppstå för företaget i en flexibel IT-miljö för personalen kan handla om att:

- Lösenord används utan större eftertanke och blir för svaga
- Företaget varken har kontroll eller insyn i vilka program och applikationer som laddas ner till olika terminaler
- Programvaror, routrar och operativsystem inte uppdateras regelbundet
- Backup saknas på viktig information

När ert företag skyddar sin företagsgemensamma IT-miljö behöver du även ta hänsyn till att varje anställd troligen gjort en egen anpassning och se det som en helhet för att minimera riskerna.

- Riktlinjer för hur lösenord hanteras, det vill säga att starka lösenord väljs och byts ut regelbundet
- Kontroll över vilka program, applikationer och mjukvara som laddas ner till olika terminaler
- Håll programvaror, routrar och operativsystem uppdaterade
- Kontrollera att varje individ i företaget uppdaterar virusskydd och brandväggar
- Identifiera vilken information som den anställde behöver göra backup på regelbundet
- Fundera på vem som har behörighet till vilken information, inför eventuell behörighetskontroll
- Säkerställ att företags- och privatrelaterade konton samt utrustning hålls separerade
- Påminn regelbundet om riskerna, gå igenom riktlinjerna och hur personalen ska agera

Den anställda

Det mänskliga beteendet är den enskilt största riskfaktorn för företag. Det är också den faktor som är svårast att ändra på och därmed att skydda sig emot. Kraven på individens eget ansvar ökar, särskilt hos mindre företag. Individens medvetenhet om sitt eget beteende behöver höjas.

Den anställdas privata IT-miljö och företagets IT-miljö flyter många gånger ihop. Ni kanske har anställda som arbetar på olika platser, ibland från hemmet och kanske från fritidshuset eller närmaste café. Utrustning och program som ert företag tillhandahåller utnyttjas för privata ändamål och vice versa. Det betyder att ni som företag bara delvis kontrollerar den anställdes IT-miljö och betydelsen av att den anställde tar ett eget ansvar blir stor. Den enskildes bristande kunskap kring IT-säkerhet anses idag vara den svagaste länken i ett företags säkerhetsarbete och svårast att lösa enbart tekniskt.

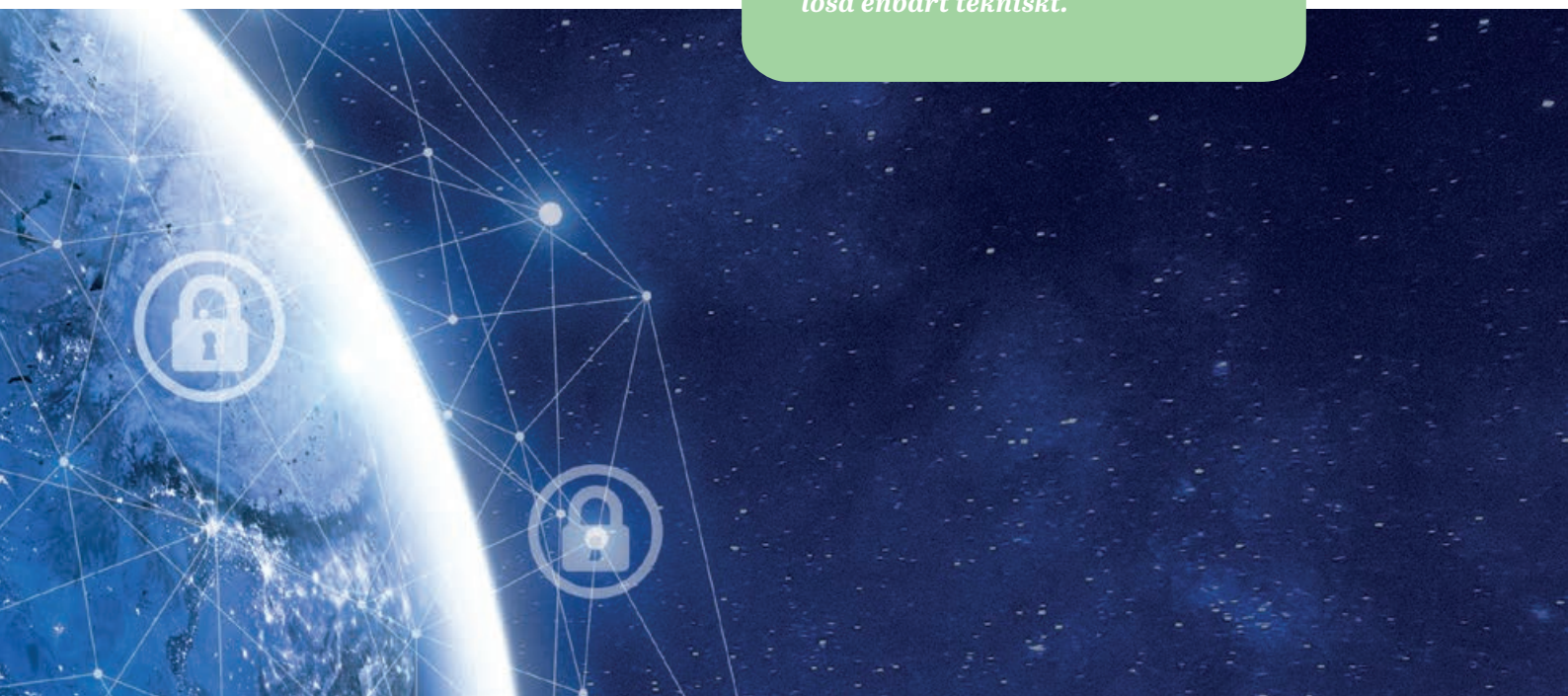
Vanliga riskområden är:

- Publika, oskyddade, nätverk som den anställda använder
- Besök på oseriösa hemsidor och hantering i sociala medier
- Riskfylld hantering av internetköp
- Länkar i mail och att meddelanden med skadlig kod öppnas
- Företagskänslig information skickas från företaget utan säkerhet
- Mailadress eller mailbox blir kapad
- Nedladdning av skadliga appar och program
- Anslutning av fysiska tillbehör som sprider virus

Att skydda sig handlar mycket om beteende och medvetenhet. Den anställda behöver bli informerad och påmind om vilka risker som finns och vad företaget har för riktlinjer. Den behöver bli påmind om att:

- Följa företagets riktlinjer för IT-säkerhet
- Reflektera över vilken infrastruktur som används i olika situationer, samt vara försiktig med att använda publika och oskyddade nätverk
- Vara misstänksam om varifrån e-post kommer och när bifogade länkar/filer kommer oväntat eller från okända avsändare
- Stänga av bluetooth och internetdelning när de inte används
- Hålla programvaror, routrar och operativsystem uppdaterade
- Använda lösenord för all utrustning
- Hålla koll på hur känslig information lagras och kryptera känslig information
- Se till att utrustningen, programvara, routrar, virusskydd, brandväggar och appar är uppdaterade med den senaste versionen
- Vara försiktig med vilka externa tillbehör som ansluts till utrustningen
- Reflektera över beteendet på hemsidor, sociala medier, hantering av vänförfrågningar, deltagande i särskilda grupper etcetera

Den enskildes bristande kunskap kring IT-säkerhet anses idag vara den svagaste länken i ett företags säkerhetsarbete och svårast att lösa enbart tekniskt.



Om du vill läsa mer

Det finns mycket information på sidan **https://www.informationssakerhet.se** som är bra för företag som vill arbeta med och öka sin egen IT- och cybersäkerhet. Nedan finns några exempel från den sidan samt från Stöldskyddsföreningen och National Cyber Security Centre i UK.

- Informationssäkerhet för små företag, rekommendationer för dig som driver eget företag med upp till 10 anställda. Myndigheten för samhällsskydd och beredskap (MSB) **https://www.informationssakerhet.se/stod--vagledning/saker-hantering-av-information2/informationssakerhet-sma-foretag/**
- Metodstöd för systematiskt informationssäkerhetsarbete, en översikt. Myndigheten för samhällsskydd och beredskap (MSB) **https://www.informationssakerhet.se/metodstodet/**
- SSF Cybersäkerhetsarbete Bas, Sammanfattning och definitioner. Stöldskyddsföreningen (SSF) **https://www.stoldskyddsforeningen.se/foretag/utbildningar/ssf-cybersakerhet-bas---grundlaggande-it-sakerhet/**#
- Cyber Security: Small Business Guide. National Cyber Security Centre. **https://www.ncsc.gov.uk/collection/small-business-guide**

Teknikföretagen kan även rekommendera verktyg och kurser för våra medlemsföretag.

VAD GÖR TEKNIKFÖRETAGEN INOM DIGITALISERING

Med digitalisering avses de nya möjligheter, utmaningar och konsekvenser som uppkommer genom framsteg inom elektronik, informationssystem och kommunikationsteknik. Rätt nyttjad kan digitaliseringen medföra att industrin kan höja produktiviteten, nå större marknader, sänka kostnader och samtidigt skapa nya produkter, affärsverksamheter och arbetstillfällen.

Teknikföretagen bevakar, driver och påverkar frågor inom digitalisering utifrån våra medlemsföretags behov. Har ni frågor kontakta:

Maria Rosendahl, Enhetschef, Kompetensförsörjning och Digitalisering
maria.rosendahl@teknikforetagen.se, tfn 08-782 09 77

Patrik Sandgren, Expert Digitalisering
patrik.sandgren@teknikforetagen.se, tfn 08-782 09 42

Skydda din IT-miljö

EN GUIDE TILL MEDVETET
SÄKERHETSARBETE I MINDRE TEKNIKFÖRETAG

Teknikföretagen

Teknik gör världen bättre
Den svenska teknikindustrins företag står för de lösningar som tacklar vår tids stora utmaningar.
Det är hos Teknikföretagen som dessa företag är medlemmar.

2019. FORM: ORDFÖRRÅDET. FOTO: SHUTTERSTOCK. TRYCK: GEFAB.