Hur säkrar vi den svenska

kompetensen inom cybersäkerhet?

SOFF
Säkerhets- och försvarsföretagen

Cyberhotet kommer från stater

Demaskop-panelen från i februari konstaterade att svenskarna ser cyberhotet som ett större hot mot Sveriges säkerhet än både världsekonomin och klimatet. Det är inte obefogat. Det statsunderstödda cyberspioneriet mot företag, myndigheter och forskningsaktörer har växt dramatiskt de senaste tio åren.

SAMHÄLLET STÅR INFÖR en enorm förändring när produkter och tjänster kopplar upp sig mot varandra. På samma gång som mängden affärskritiska och värdefulla data växer med 5G, uppkopplade enheter, förmågan att hantera stora mängder data och artificiell intelligens ökar även risken. Sammankopplingen mellan exempelvis telekomföretagens nätverk och företagens värdeskapande affärsprocesser blir tätare vilket ytterligare sporrar cyberspioneri.

FÖR DET ÄR LÖNSAMT att spionera. Det är dessutom riskfritt då det saknas internationell rätt som förhindrar cyberspionagen. Därför växer det statsunderstödda cyberspionaget. Genom att spionera på företag – och på så sätt komma över information och affärsdata – kan angriparländerna hjälpa inhemska företag att snabbare utveckla nya produkter och tjänster till en global marknad. För Ryssland, Kina och andra är cyberspioneri ett tillåtet verktyg att använda för att konkurrera och för att utöva staternas inflytande. Hotet kommer därför från stater och statsunderstödda aktörer. Inte enskilda hackare.

SÅRBARHETER, BEROENDEN OCH RISKER kommer vi inte ifrån. Det går inte att helgardera sig. Det handlar om att utveckla strategier, verktyg och tjänster som behövs för att höja vår förmåga. Inte minst för att värdera risk och

Det handlar om att utveckla strategier, verktyg och tjänster som behövs för att höja vår förmåga.

effekt. Det är en kapplöpning mot den svagaste länken.

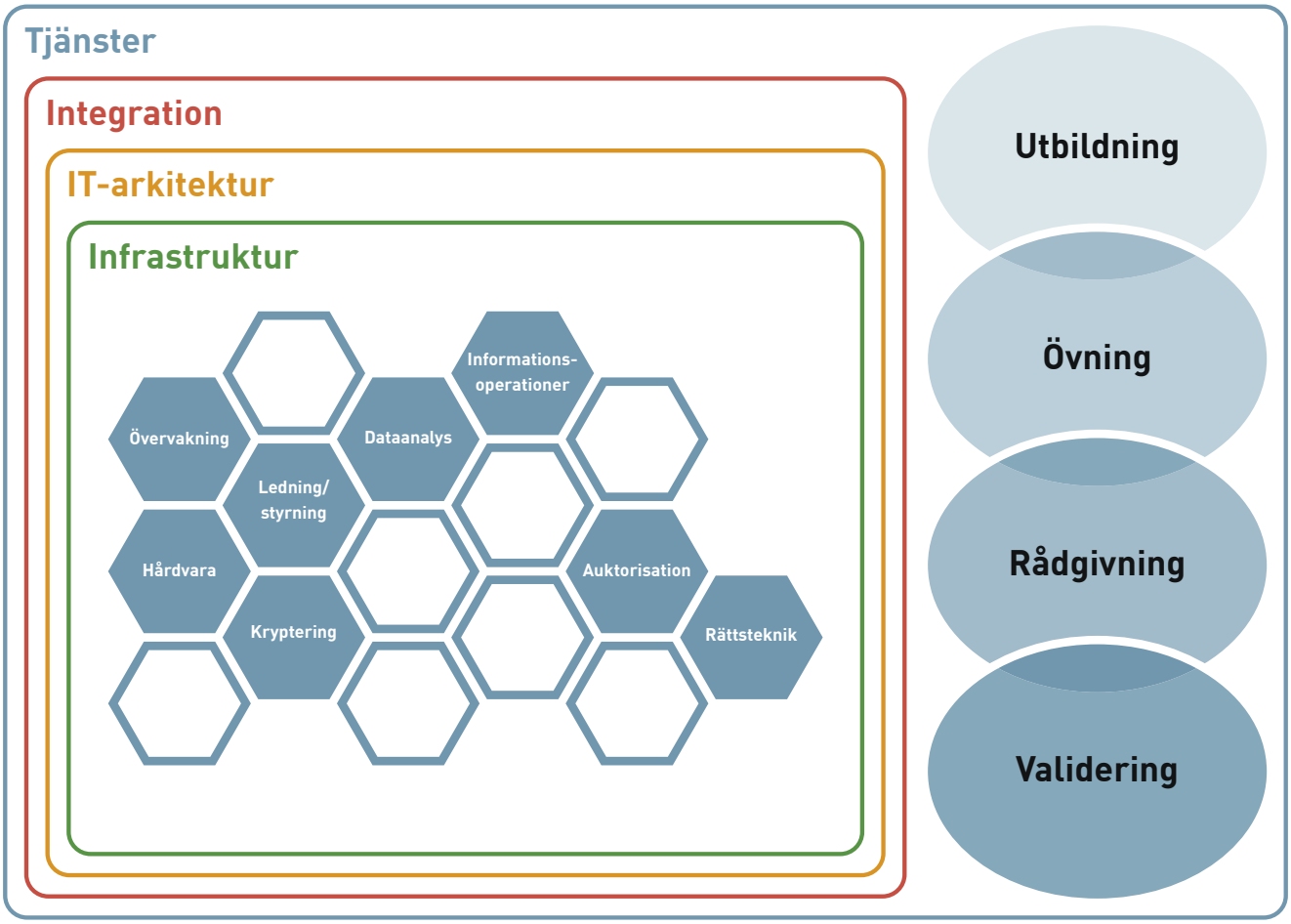
SKYDD AV DET DIGITALA samhället är dock inte ett ansvar för regeringen allena och kan inte lämnas till staten att ensamt bygga upp. Eftersom våra utmaningar är mångfacetterade, måste vi arbeta tillsammans för att skydda det som ska skyddas och hjälpa varandra att hantera de risker som vi känner till – och de vi inte känner till. Idag ligger en stor del av hotet i aningslöshet och i den mänskliga faktorns brister. Vi måste samtidigt fortsatt verka för att normer, tydliga röda linjer, gemensam terminologi och ömsesidigt förtroendeskapande åtgärder växer fram.

VÅR FRAMGÅNG ATT MÖTA cyberhot handlar till stor del om ny innovation; men då inte bara tekniska lösningar utan modeller för samverkan mellan berörda aktörer.

LÄS MER!

För att öka medvetenheten och kunskapen samlar föreningen intressanta och relevanta publikationer på området. På engelska har vi även tagit fram en sammanfattning av olika publikationer.

CYBERMARKNADENS UTVECKLING



Verksamhetsområden inom vilket SOFF:s medlemsföretag erbjuder tjänster och lösningar.

De senaste fem åren har SOFF:s medlemsföretag inom cybersäkerhet redovisat **en ökning i omsättning på mellan 6-18% per år**. Bedömningen är att tillväxten kommer att öka på både kort och lång sikt.

Den enskilt mest dimensionerande faktorn för tillväxt är **tillgången till kompetens.**

Betydelsen av kryptografi

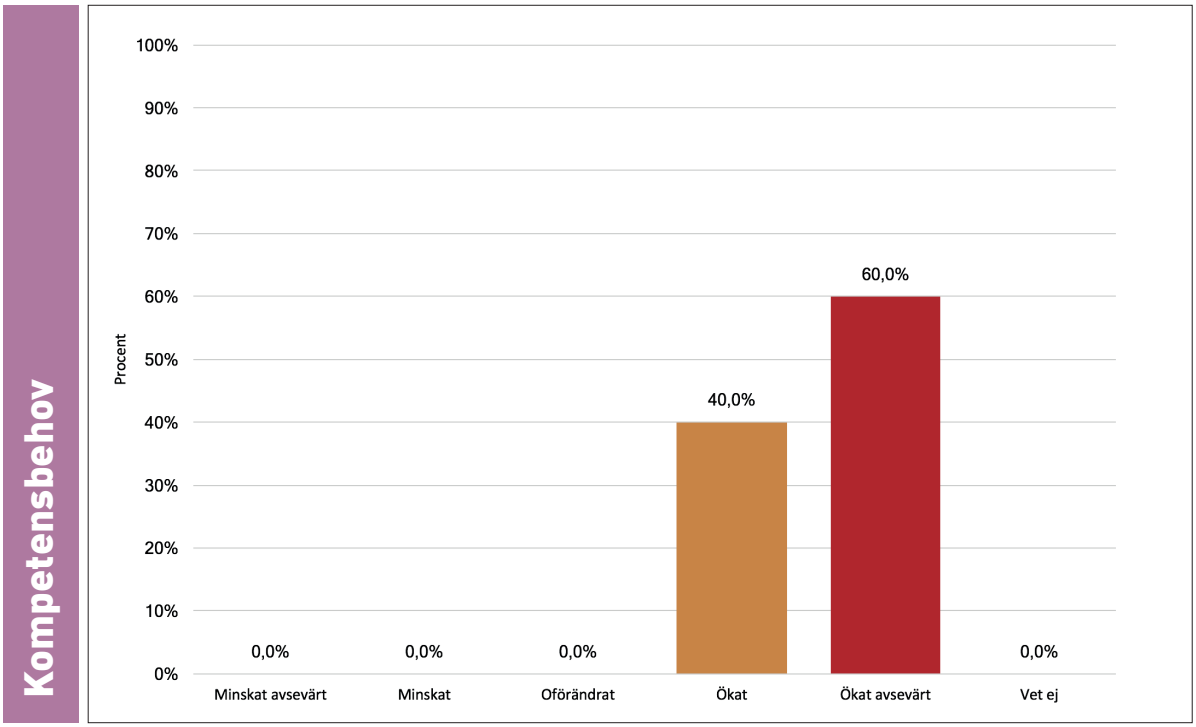
Av särskilt intresse är att staten har tillgång till teknik som av särskilda sekretesskäl har ett betydande nationellt intresse eller skydds-värde. Genom att kryptera information blir den svårare att avlyssna eller på annat sätt ta del av och för samhällets säkerhet berör denna förmåga flera olika samhälls-aktörer.

Läs mer om krypto på www.soff.se

Behovet av kompetens – och varifrån

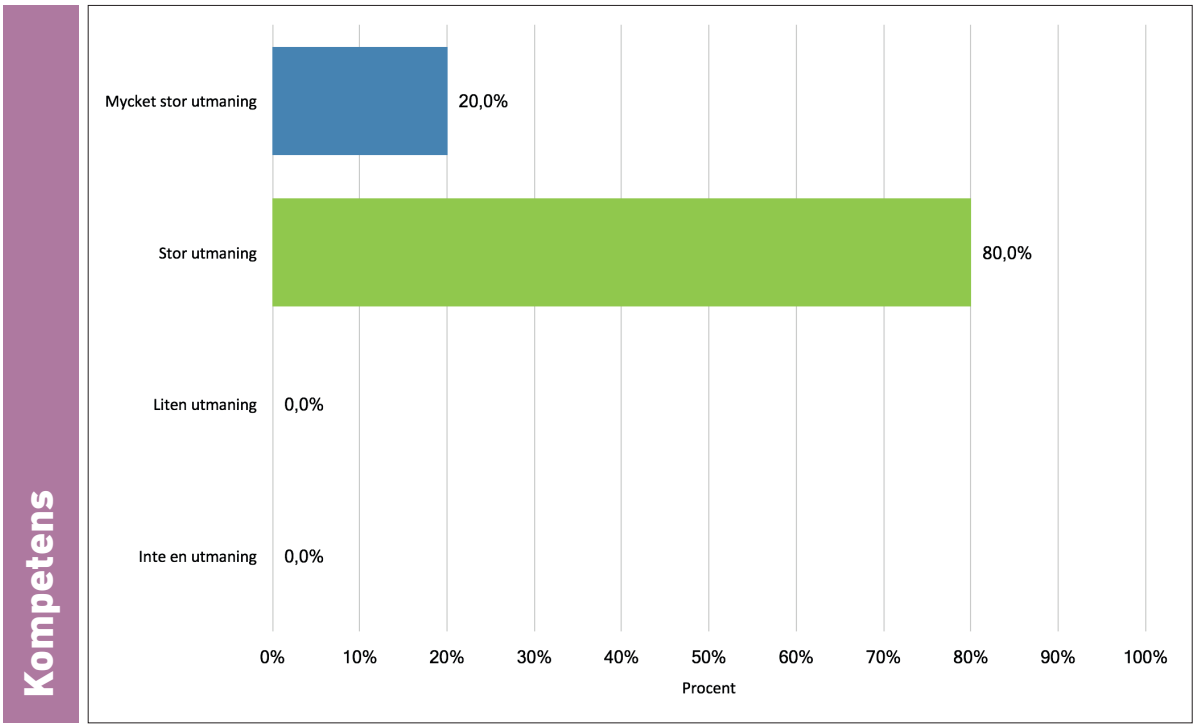
SOFF genomförde i maj 2018 en undersökning av behovet av cybersäkerhetskompetens hos våra medlemsföretag. Syftet var att bättre förstå hur företagen idag säkrar sin kompetens och vilket behov de ser framöver.

SOFF:s medlemsföretag anger att behovet av nya medarbetare med cybersäkerhetskompetens har ökat avsevärt under de senaste åren. I snitt anger företagen att behovet (skala 1-5) ökat med 4,6. I jämförelse med andra yrkeskategorier av ingenjörer är detta unikt.

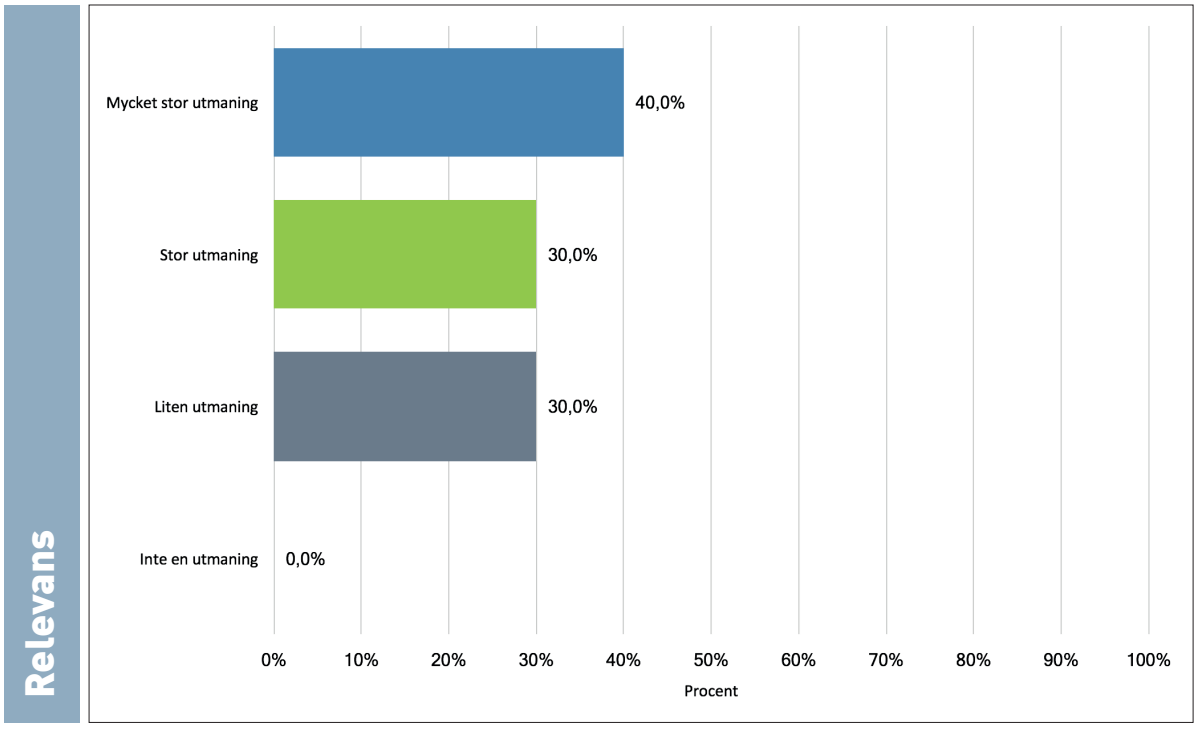


Kompetens. Många sökande saknar den formella kunskapsnivå som företagen behöver.

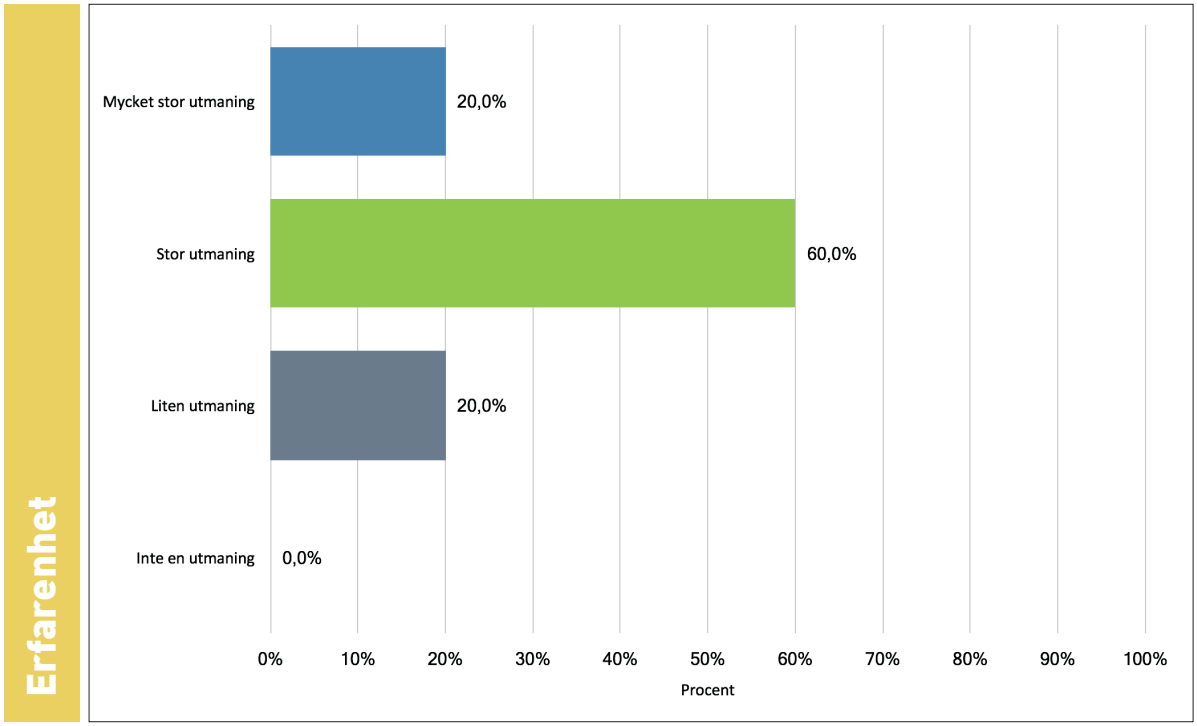
Företagen ser tre olika typer av utmaningar avseende kompetensförsörjningen och även om företagen rangordnar utmaningarna enligt nedan, skiljer det procentuellt ändå lite mellan de tre.



Kompetens. Många sökande saknar den formella kunskapsnivå som företagen behöver.



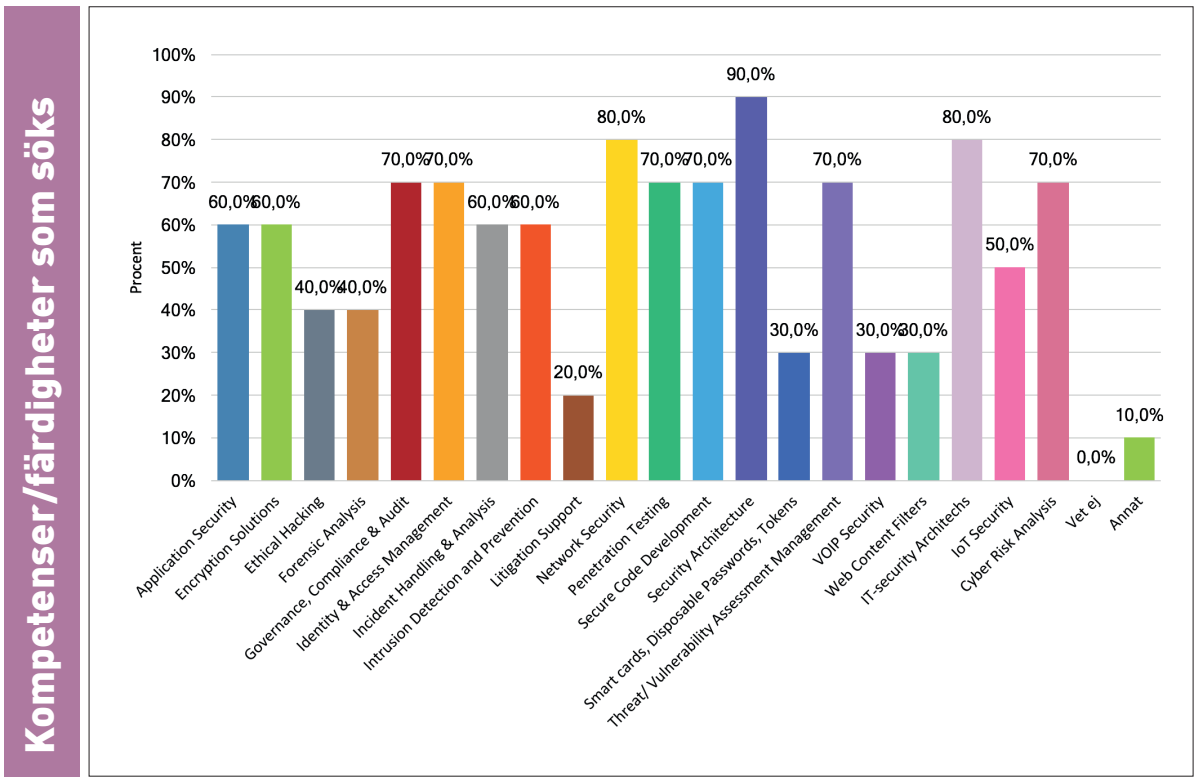
Relevans. Utbildningarna anpassas inte tillräckligt snabbt för att relevant möta marknadens behov som utvecklas tekniskt snabbt.



Erfarenhet. Många sökande saknar den nivå av yrkeserfarenhet som företagen förväntar sig.

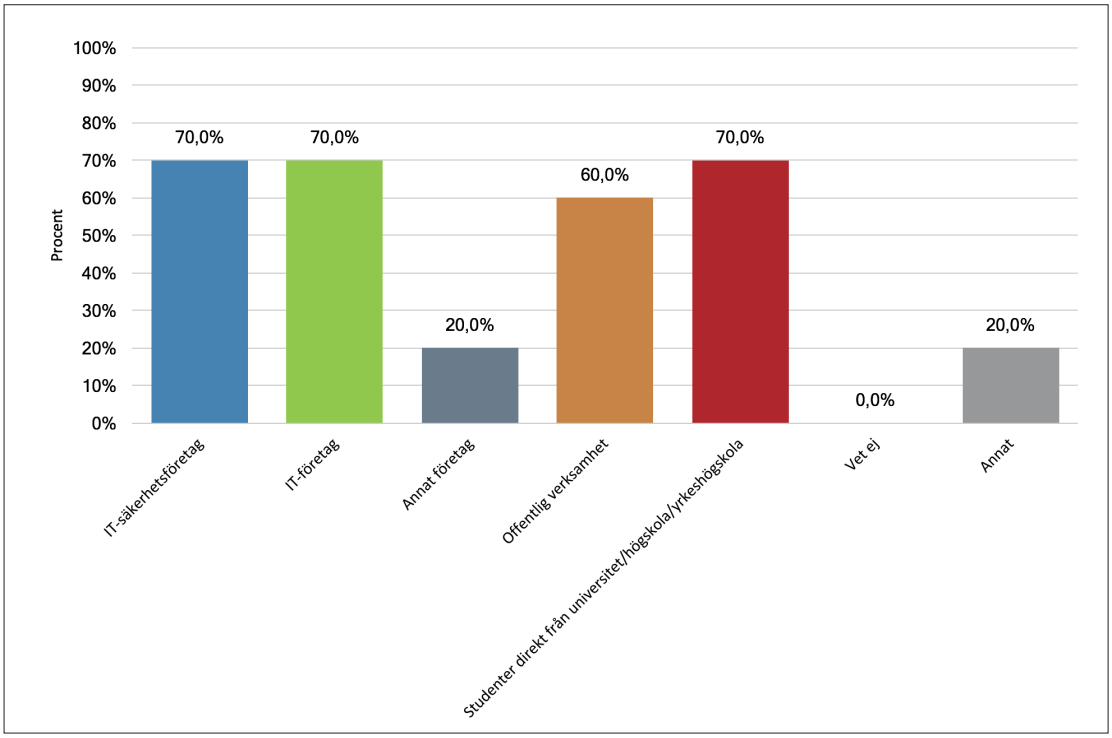
Företagen söker kompetenser/färdigheter inom många områden. SOFF:s undersökning visar att fler än 2/3 av deltagande företag söker expertis inom fler än 18 olika specialistkompetenser. Mest eftertraktat är kompetenser inom områdena **Security Architecture**, **IT-security Architechs** och **Network Security**.

Andra är **Governance**, **Compliance & Audit**, **Identity & Access Management**, **Penetration Testing**, **Secure Code Development**, **Threat/ Vulnerability Assessment Management** och **Cyber Risk Analysis**.



Företagen letar efter nya medarbetare **främst hos andra IT-företag**, men även andra **cybersäkerhetsföretag**. De söker även aktivt på **högskolorna**.

Arbetsgivare man letat hos



Ovanligt få företag känner dock till de utbildningar inom IT-säkerhet som erbjuds och få känner igen utbildningarna från sina rekryteringar. De utbildningar som företagen mest känner igen är IT-forensik och informationssäkerhet på Högskolan i Halmstad, Civilingenjör i datorsäkerhet vid Blekinge tekniska högskola, Nätverkssäkerhetutbildningen på Linnéuniversitetet samt masterprogrammet i informationssäkerhet vid Stockholms universitet. Den senare är den i särklass mest välkända hos företagen.

Utbildningar

Inför Cyberkompetensdagen den 17 oktober kommer vi att presentera en inventering av samtliga IT-säkerhetsutbildningar i den mån information är tillgänglig. Delanalysen visar på stora utmaningar;

- **För få utbildningar**
  Se listning nedan
- **För få genomför utbildningen**
  Exempel från en grundutbildning:
- **För få kvinnor**
  Andelen kvinnor som avslutar utbildningar är färre än 10%.
- **För få med svenskt medborgarskap**
  Kompetensen stannar inte i Sverige

Antal sökande: **668**
Antal antagna: **90**
Antal examinerade: **10**

Kommentar: Många kurser har stora avhopp. En del slutar tidigt för att de inte klarar av kurserna, ofta klarar de inte matematiken eller programmeringen eller finner att det inte är rätt utbildning. Många får jobb innan de är färdiga. Inte alla av de som klarat utbildningen begär ut en examen.

Relevanta cybersäkerhetsutbildningar

1. GRUNDNIVÅ – upp till kandidatexamen

1.1 IT-forensik och informationssäkerhet
180 högskolepoäng, Högskolan i Halmstad
Studieort: Halmstad

1.2 Nätverkssäkerhet
180 högskolepoäng, Linnéuniversitetet (Kalmar Växjö)
Studieort: Växjö

2. AVANCERAD NIVÅ - Magister eller Masterexamen

2.1 Masterprogram i informationssäkerhet
120 högskolepoäng, Stockholms universitet
Studieort: Stockholm

2.2 Informationssäkerhet, master
(Normal, samt på Distans, Luleå)
120 högskolepoäng, Luleå tekniska universitet
Studieort: Luleå

2.3 Magisterprogram i nätverksforensik
60 högskolepoäng, Högskolan i Halmstad
Studieort: Halmstad

2.4 Masterprogram i informatik
– ledning och styrning av informationssäkerhet
120 högskolepoäng, Örebro universitet
Studieort: Örebro
Startar hösten 2018

2.5 Masterprogram i informatik – ledning och styrning av informationssäkerhet
120 högskolepoäng, Högskolan i Skövde
Studieort: Skövde
Startar hösten 2019

3. GRUNDNIVÅ samt AVANCERAD

3.1 Civilingenjör i datorsäkerhet
300 högskolepoäng, Blekinge tekniska högskola
Studieort: Karlskrona

4. KURSER

4.1 Mobil och trådlös säkerhet, Linnéuniversitetet 7,5hp

4.2 Internetsäkerhet, Linnéuniversitetet,
Engelska distans 7,5hp

4.3 Datasäkerhet I, Karlstad universitet 7,5hp

4.3 Ethical hacking, KTH 7,5hp

Relevanta cybersäkerhetsutbildningar - fortsättning

5.0 YH-utbildningar

5.1 IT-säkerhetstekniker
400 YH-poäng, Campus i12, Studieort: Eksjö

5.2 IT-säkerhetstekniker
440 YH-poäng, Iftac, Studieort: Hudiksvall

5.3 IT-säkerhetstekniker
2 år, Newton, Studieort: Stockholm, Göteborg

5.4 IT-säkerhetstekniker
400 YH-poäng, Frans Schartaus Handelsinstitut, Studieort: Stockholm

5.5. IT-säkerhetsspecialist
400 YH-poäng, Stockholms Internationella Handelsskola, Studieort: Malmö samt Stockholm

5.6 IT-säkerhetsspecialist
400 YH-poäng, Xenter, Studieort: Tumba

5.7 Informationssäkerhetssamordnare
3 terminer, Företagsuniversitetet, Studieort: Stockholm

Sammanfattning

- Det är inte en rent utbildningspolitisk fråga. Den har **betydande försvars- och säkerhetspolitiska implikationer**.
- Antalet sökande och antalet platser ökar, men för långsamt när samtidigt efterfrågan på IT-säkerhetskompetens exploderat och hittills varit eftersatt.
- Problemet går inte enbart att lösa med utbildningsinsatser.