FSPOS

Finansiella Sektorns Privat-
Offentliga Samverkan

Cyber Awareness
– att höja kunskapen om cyberrisker

Version: 2018-12-06
FSPOS Fokusgrupp Cybersäkerhet

Inledning

Den globala kostnaden för bristande kunskap om cybersäkerhet (Cyber Awareness) uppskattas av Europeiska rådet till 400 miljarder euro om året[1]. National Institute of Technology (NIST) belyser hur phisning, social engingeering och skadlig kod framgångsrikt utnyttjas av angripare; *"Some of the most effective current attacks on cyber networks world-wide exploit user behaviour."*[2]. Att öka kunskaperna om cyberrisker är av stor vikt för företag och organisationer verksamma inom den finansiella sektorn.

Mot bakgrund av det ökade behovet har FSPOS studerat hur organisationer arbetar med Cyber Awareness för att dela goda exempel. Dagens hotbild i kombination med bristande kunskap gör Cyber Awareness till ett prioriterat område för FSPOS medlemmar.

Syftet med Cyber Awareness är att medvetandegöra anställda om regelverk för cybersäkerhet, den aktuella riskbilden samt belysa hur organisationen ska hantera cyberrisker[3]. Enligt The European Council har 69% av alla företag en grundläggande eller bristfällig förståelse för sin exponering mot cyberrisker[4]. Organisationer verksamma inom den finansiella sektorn har dock generellt sett en högre kunskapsnivå enligt många källor. Forskare kopplade till MSB projektet SECURIT presenterade nyligen en undersökning som jämför informationssäkerhetskulturen mellan sex branscher; sjukvård, socialtjänst, högskola, IT, bank och kemisk tillverkningsindustri. Studien visade att *"Banksektorns profil avvek kraftigt positivt från genomsnittet."*[5]. Vidare visar SANS Institute (SANS) att finans- och banksektorn uppnår mognadsnivå tre i deras femgradiga skala[6], *"Promoting Cyber Awareness and behaviour change"*.

Innehållet i denna PM baseras på information från föreläsningar, möten i FSPOS fokusgrupp samt litteraturkällor.

Syfte

Syftet med detta dokument är att beskriva hur organisationer inom den finansiella sektorn kan arbeta med Cyber Awareness. Genom att beskriva olika metoder för Cyber Awareness-arbete kombinerat med ett årsprogram utgör dokumentet en beskrivning av god praxis.

---

1 https://www.consilium.europa.eu/en/policies/cyber-security/
2 NIST Special Publication 800-16 Revision 1 (3rd Draft), (2014), A Role-Based Model for Federal Information Technology/Cybersecurity Training, Sid. 7
3 CRR Supplemental Resource Guide Volume 9 (2016), Training and Cyber Awareness Version 1.1 (2016), Carnegie Mellon University (funded and supported by Department of Homeland Security and United States Department of Defense.), sid. 5-6.
4 https://www.consilium.europa.eu/en/policies/cyber-security/
5 Informationssäkerhet och Organisationskultur, (2017), Studentlitteratur, Hallberg, Johansson, Karlsson, Lundberg, Lundgren, Törner, Sid. 50
6 SANS Security Cyber Awareness Report (2018) Building Successful Security Cyber Awareness Programs, Sid 12.

Metoder för Cyber Awareness

Det går att arbeta med Cyber Awareness på flera olika sätt. För att uppnå ett bra slutresultat är det viktigt att metoden anpassas efter organisation och målgrupp[7]. På en övergripande nivå kan metoderna delas upp i två områden; utbildning och organisationsinterna forum för informationsdelning.

Utbildning är en metod som genom strukturerade och handledda insatser i fysiska eller digitala rum höjer kunskapen om cyberrisker och hur de hanteras.

Organisationsinterna forum för informationsdelning är en metod som i fysiska eller digitala rum internt informerar eller möjliggör diskussion om cyberrisker och hur de hanteras.

Medlemmar ur FG Cyber använder sig av dessa metoder i kombination för att öka organisationens Cyber Awareness. Att kombinera metoderna är effektivt men också tidskrävande, varför det är nödvändigt att ha tillräckliga resurser till förfogande.

Cyber Awareness is the ability of the user to recognize or avoid behaviours that would compromise cybersecurity; practice of good behaviours that will increase cybersecurity; and act wisely and cautiously, where judgment is needed, to increase cybersecurity.
- NIST Special Publication 800-16 Revision 1 (3rd Draft), (2014), Sid. 8

Cyber Awareness is an ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organisation from lasting behavioural change.
– ENISA Cyber Security Culture in organisations (2017), sid. 40.

Figur 1. Definition av Cyber Awareness.

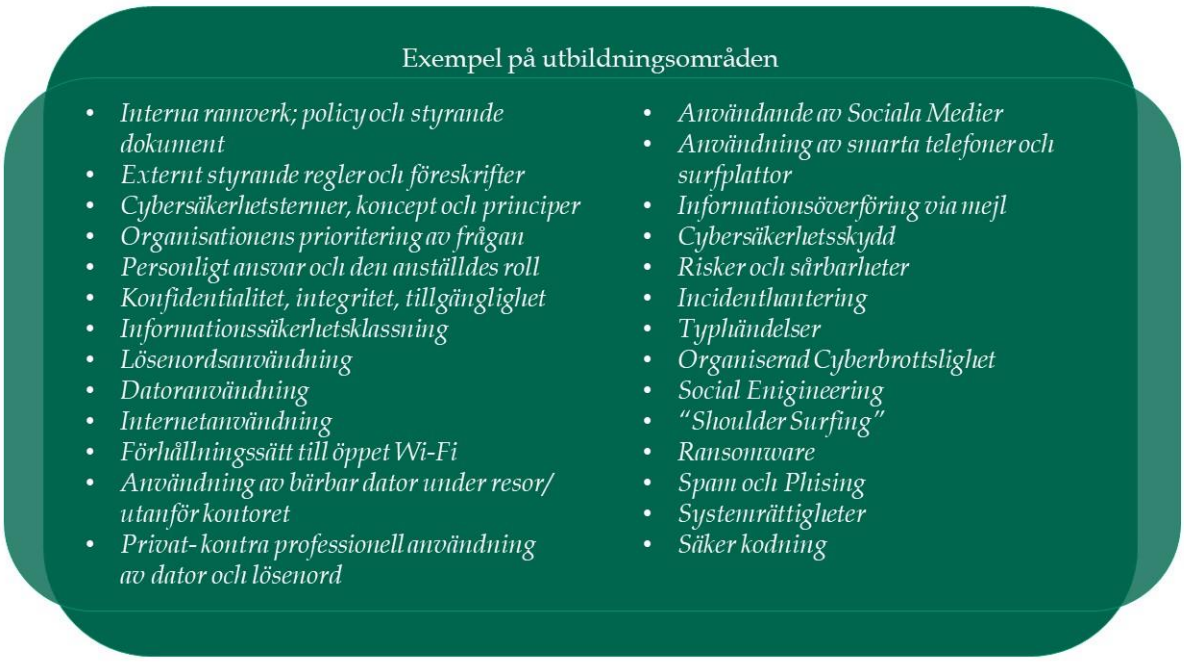
7 https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness "A one size fits all approach is not typically appropriate for many organizations",

Utbildning

Att utbilda anställda och andra personer som arbetar för organisationen är en viktig metod i arbetet med Cyber Awareness. En utbildning kan genomföras genom analoga eller digitala insatser, men behöver ha ett relevant innehåll och riktas till målgruppen. Även ENISA påpekar att framgångsfaktorer för en lyckad Cyber Awareness-utbildning är att den är relevant, en del av det kontinuerliga lärandet samt inkluderar hela organisationen och sprider entusiasm[8].

Utbildningsområden

En viktig fråga kopplat till utbildning är; *Vad ska vi utbilda inom?* Frågan om utbildningsområde bör besvaras tidigt i planeringen då den påverkar målgrupp, omfattning, fördjupning och typ av utbildning. Då cybersäkerhetsområdet är brett och riskerna många finns flera områden organisationens personal behöver utvecklad kunskap inom. Genom fokusgruppens erfarenheter och litteraturkällor[9] kan nedan exempel på utbildningsområden konkretiseras för att inspirera valet av utbildning. Figur nedan utgör en bruttolista för val av utbildningsområde.



Figur 2. Exempel på utbildningsområden.

---

8 ENISA (2017), Cyber Security Culture in organisations, Sid. 40
9 NIST Special Publication 800-16 Revision 1 (3rd Draft), (2014), A Role-Based Model for Federal Information Technology/Cybersecurity Training, Sid. 30-31
9 NIST Special Publication 800-50 (2003), Building an Information Technology Security Cyber Awareness and Training Program, Sid. 24-25

Utbildningsmålgrupper

Samtliga anställda och personer kopplade till organisationen bör utbildas om cyberrisker oavsett om de är anställda, konsulter eller leverantörer. För särskilda och fördjupade utbildningsinsatser krävs vidare en målgruppsanpassad analys.

Personer som ska erhålla utbildning kan delas upp i tre kategorier baserat på riskbild; samtliga anställda, specialister samt ledningspersonal, vilket även preciseras av PCI Security Standard Council (PCI)[10]. Vilka funktioner som kopplas till vilket område bör definieras av den egna organisationen och bör utgå från hur stor risken är att de utsätts för cyberangrepp. Syftet med att koppla funktion till riskområde är möjligheten att konkretisera utbildningsbehov därefter. Urval av personer påverkar således utbildningsbehov och utbildningskrav, vilket exemplifieras i *Figur 3. Exempel på utbildningsmålgrupper.* Exempelfunktioner i figuren är baserade på fokusgruppens erfarenheter och tillgängliga litteraturkällor[11]. En tumregel är att alla anställda bör utbildas på en grundläggande nivå vid nyanställning samt därefter var tredje år, samt att högriskgrupper bör utbildas mer frekvent på en detaljerad nivå.

Figur 3. Exempel utbildningsmålgrupper.

---

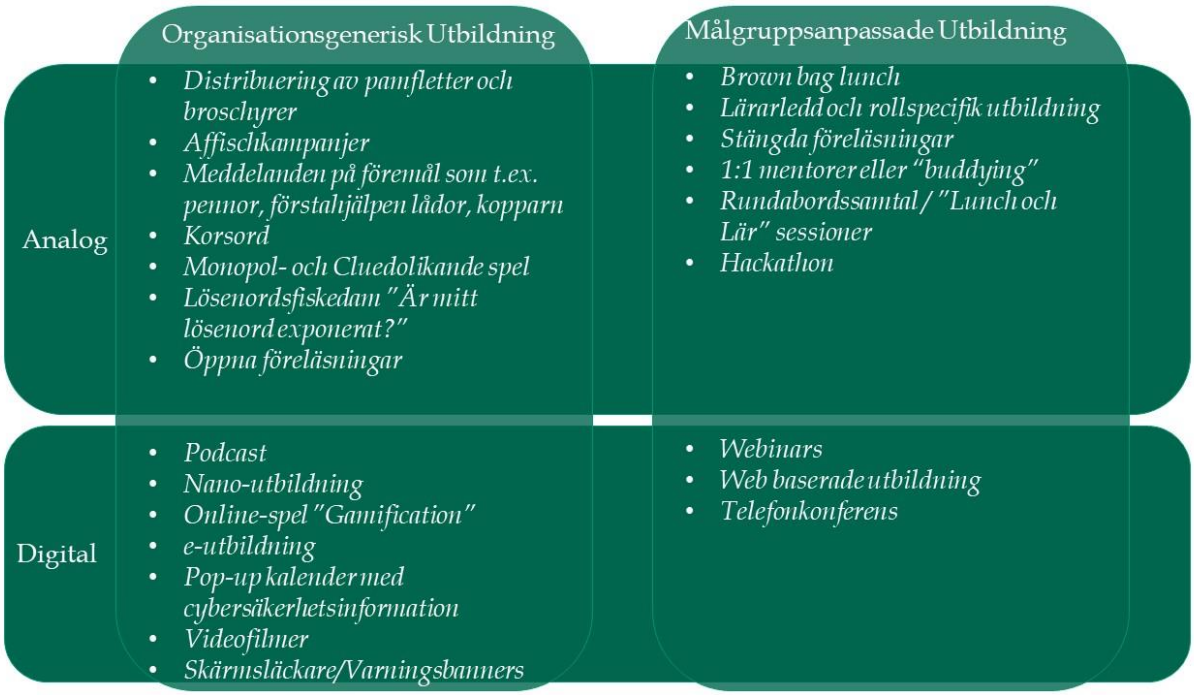
10 PCI Data Security Standard (PCI DSS) Version: 1.0 (2014), Information Supplement: Best Practices for Implementing a Security Cyber Awareness Program, Sid. 4
11 NIST Special Publication 800-50 (2003), Building an Information Technology Security Cyber Awareness and Training Program, Sid. 16, 20, 27-28.
11 PCI Data Security Standard (PCI DSS) Version: 1.0 (2014), Information Supplement: Best Practices for Implementing a Security Cyber Awareness Program, Sid. 4.
11 CRR Supplemental Resource GuideVolume 9 Training and Cyber Awareness Version 1.1 (2016), Carnegie Mellon University (funded and supported by Department of Homeland Security and United States Department of Defense), sid. 8, 20.
11 CPMI/IOSCO (2016), Guidance on cyber resilience for financial market infrastructures, avsnitt 4.5, sida 14..

Utbildningstyper

Fokusgruppens medlemmar beskriver olika typer av utbildningar och hur dessa noggrant valts ut. Det är tydligt att digitala utbildningsinsatser blandas med analoga och att valet av dem baseras på utbildningens syfte och mål[12].

När syfte och mål definierats kan alltså typ av utbildning väljas ut. Här kan den utbildande aktören välja mellan digitala och analoga utbildningar samt huruvida utbildningen kan vara generisk och genomföras för samtliga i organisationen eller om den bör vara specialanpassat efter målgrupp. Exempel på digitala och analoga utbildningar samt generiska och målgruppsanpassade finns beskrivna i figuren nedan. Val av utbildningstyp baseras vidare även på ambitionsnivå och tillgängliga resurser.

För vissa utbildningsgenomföranden, såväl digitala som analoga, finns krav på hur utbildningsmaterial presenteras och distribueras. För bästa möjliga kvalitet på utbildningsmaterial kan kommunikationsavdelningens expertkunskap med fördel utnyttjas[13].



Figur 4. Exempel på utbildningstyper.

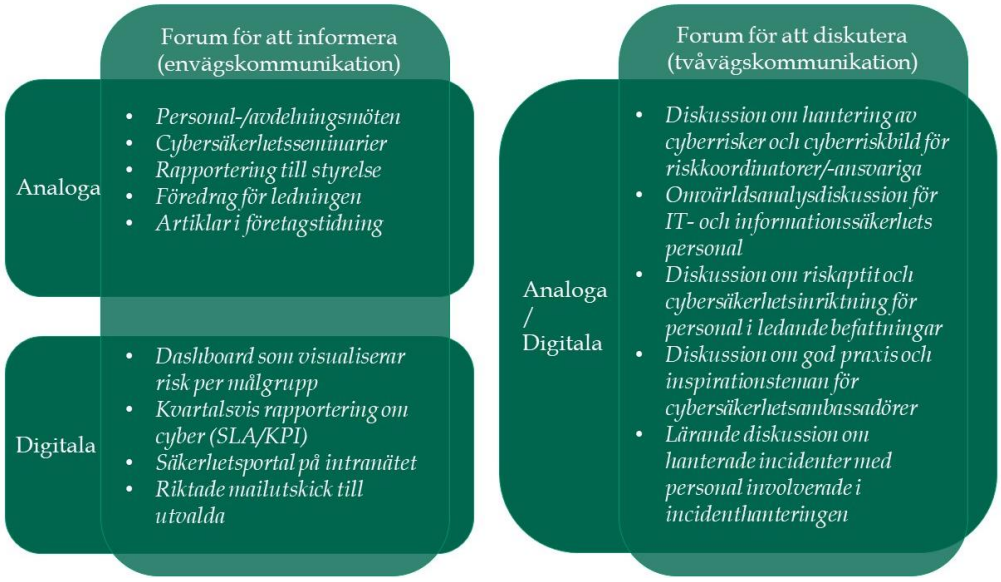
---

12 NIST Special Publication 800-50 (2003), Building an Information Technology Security Cyber Awareness and Training Program, Sid. 32-33
12 CPNI, Centre for the Protection of National Infrastructure (2017), Embedding Security Behaviours: using the 5Es – A framework for improving security behaviour within organisations, Sid. 5
12 PCI Data Security Standard (PCI DSS) Version: 1.0 (2014), Information Supplement: Best Practices for Implementing a Security Cyber Awareness Program, Sid. 21
12 CRR Supplemental Resource Guide - Volume 9 (2016), Training and Cyber Awareness Version 1.1, Department of Homeland Security (Carnegie Mellon University, United States Department of Defense), Sid. 11
13 SANS Security Cyber Awareness Report (2018), Building Successful Security Cyber Awareness Programs, Sid 23.

Organisationsinterna forum för informationsdelning

Organisationsinterna forum för informationsdelning avser analoga eller digitala platser för att informera eller diskutera cybersäkerhetsrelaterade frågor internt. Beroende på hur och vad som ska kommuniceras kan forum väljas. Nedan presenteras exempel på forum exemplifierade av fokusgruppens medlemmar samt befintlig litteratur[14]. Vid dessa forum kan personal med olika befattningar diskutera och upplysa(s) om cybersäkerhet. Här informeras forumdeltagarna kontinuerligt om risker, händelser och åtgärder kopplade till cybersäkerhetsarbetet. Dessa återkommande inslag i vardagen gör att de anställda blir en del av cybersäkerhetdialogen och tillåts själva bidra till en utvecklad förmåga, dvs de anställda blir därmed en del av ett proaktivt cybersäkerhetsarbete.

På samma sätt som en organisation gör ett strategiskt urval av personer som bör utbildas inom olika områden, så bör även ett urval göras för deltagande i dessa forum. Syfte, tema och agenda per forum och tillfälle varierar och kan enligt en av fokusgruppens medlemmar delas upp i fem teman; skydda din information, skydda din arbetsmiljö, skydda din dator, skydda dina mobila enheter samt skydda dig själv.



Figur 5. Exempel på organisationsinterna forum för informationsdelning.

För vidare läsning om informationsdelning - se FSPOS PM ”Informationsdelning av cyberrisker inom finansiell verksamhet”[15].

---

14 SANS Security Cyber Awareness Report (2018), Building Successful Security Cyber Awareness Programs, Sid 24.
14 CRR Supplemental Resource Guide - Volume 9 (2016), Training and Cyber Awareness Version 1.1, Department of Homeland Security (Carnegie Mellon University, United States Department of Defense), Sid. 11
14 CPNI, Centre for the Protection of National Infrastructure (2017), Embedding Security Behaviours: using the 5Es – A framework for improving security behaviour within organisations, Sid. 7
14 NIST Special Publication 800-50 (2003), Building an Information Technology Security Cyber Awareness and Training Program, Sid. 24-25 och 32-33
14 CPMI/IOSCO (2016), Guidance on cyber resilience for financial market infrastructures, avsnitt 9.2, sida 22.
15 http://www.fspos.se/siteassets/fspos/rapporter/2018/informationsdelning-av-cyberrisker-inom-finansiell-verksamhet.pdf

Cyber Awareness-program

Genom ett systematiskt arbete med Cyber Awareness kan organisationens resurser optimeras. Vidare kan aktiviteter genomföras med en långsiktig horisont i syfte att nå en högre mognadsnivå. I detta avsnitt beskrivs hur ett program för Cyber Awareness kan planeras, organisationsanpassas och genomföras. Exemplet baseras på erfarenheter från fokusgruppen och tillgänglig litteratur.

Programförberedelser

Att utförligt förbereda Cyber Awareness-programmet innebär bl.a. att utbildningsinsatser, aktiviteter för intern informationsdelning samt tester strategiskt väljs ut och sprids över året. Under programförberedelserna bör tre punkter[16] enligt nedan konkretiseras.

Säkerställ internt stöd och support: Det interna stödet är avgörande för ett lyckat program och det bör förankras högt upp i organisationen[17]. För ett bra resultat bör ledningspersonal även kommunicera frågans prioritet i organisationen. Som exempel kan nämnas att en organisations obligatoriska cybersäkerhetsutbildning (e-utbildning) inleds med ett anförande av VD.

Etablera en programstrategi: Programstrategin bör utgå från organisationens mål, värderingar och prioriterade område. Baserat på konkreta mål kan programmets resultat följas upp och arbetet ständigt förbättras. När mål fastställts och förankrats i de övergripande organisationsmålen kan programaktiviteter förberederas. Under det strategiska arbetet bör redan befintliga Cyber Awareness-aktiviteter identifieras och analyseras mot vad organisationen nu önskar åstadkomma, detta för en effektiv allokering av befintliga resurser. Vidare bör programmet även kopplas till ett övergripande ramverk för cybersäkerhet i de fall ett sådant finns.

Etablera en genomförandemetod: Vid arbetet med att etablera metoden för genomförande bör frågorna *vilka aktiviteter vill vi genomföra*, *vad ska vi göra internt och till vad ska vi ta hjälp av leverantörer?* besvaras. När frågorna besvarats bör ansvar fastställas för varje enskild aktivitet. Därefter kan arbetet med att planera och förbereda aktiviteterna påbörjas.

---

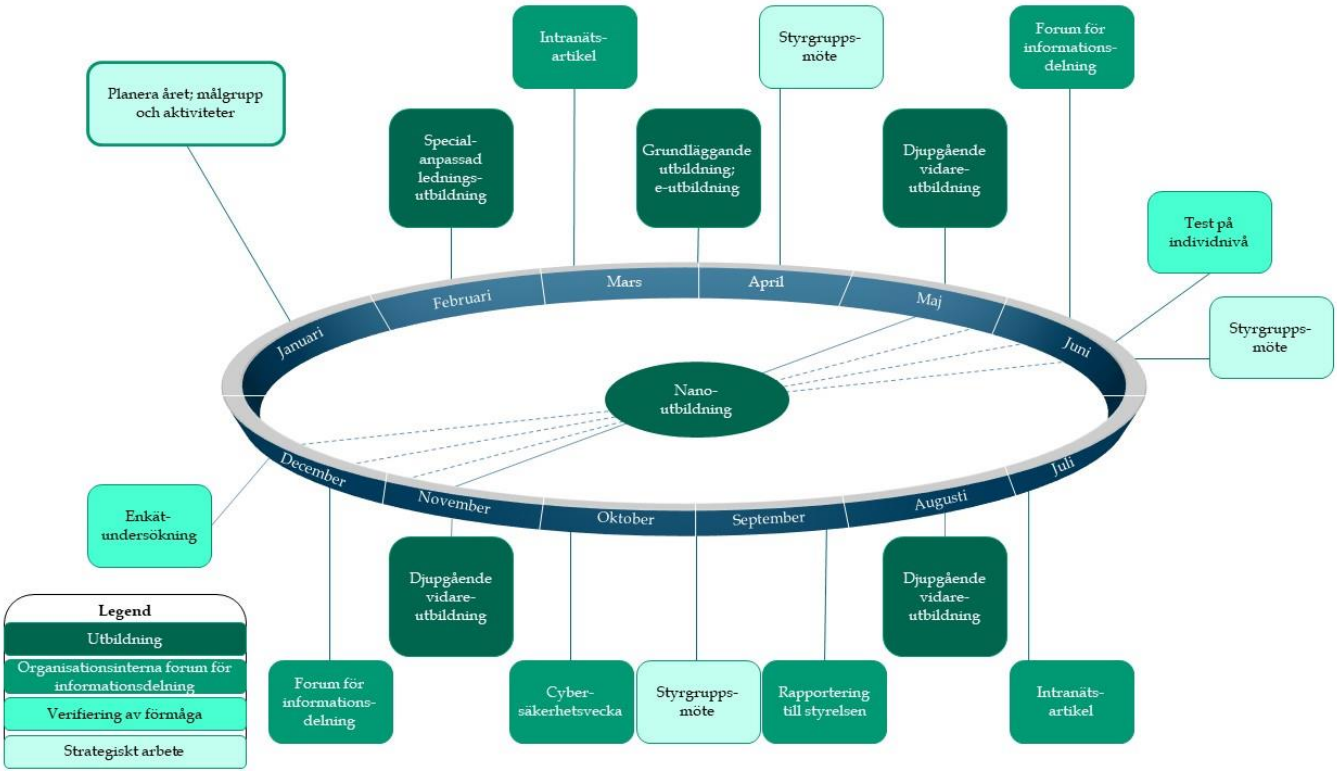
20 CRR Supplemental Resource Guide - Volume 9 Training and Cyber Awareness Version 1.1, Department of Homeland Security (Carnegie Mellon University, United States Department of Defense), Sid. 6
20 NIST Special Publication 800-50 (2003), Building an Information Technology Security Cyber Awareness and Training Program, Sid. 1, 11-12 och 31.
17 CPMI/IOSCO (2016), Guidance on cyber resilience for financial market infrastructures, avsnitt 2.3.2, sida 10.

Programgenomförande

Givet att det kontinuerliga arbete med Cyber Awareness är tids- och resurskrävande samt att aktiviteter behöver förberedas i god tid kan det vara en god idé att definiera en årscykel att arbeta efter. Genom att besluta om aktiviteter i förväg (utbildning, organisationsinterna forum för informationsdelning, verifiering av förmåga, strategiskt arbetet) samt datum för genomförande kan arbetet ske med god framförhållning och med bättre kvalitet.

Det exempel som presenteras nedan är ett förslag hur aktiviteter kan fördelas under en 12-månaders period.

I det illustrativa exemplet har nämnda aktiviteter fördelats ut under ett år. Det illustrativa exemplet följs av en beskrivande text *Exempel – beskrivning Cyber Awareness-årscykeln.*



Figur 6. Årscykel för Cyber Awareness-program.

Exempel – beskrivning Cyber Awareness-årscykel

Datum	***Aktivitet***	***Beskrivning***
Januari	*Planera året; Målgrupp och aktiviteter*	Uppstartsmöte där en styrgrupp konkretiserar aktiviteter och utdelar ansvar. Områden att definiera är: 1) utbildningsområden 2) målgrupper samt 3) utbildningstyper.
Februari	*Specialanpassad ledningsutbildning*	Koncernsäkerhetschef genomför en rollspecifik utbildning för ledningsgruppen på temat Interna ramerk; Policy och styrande dokument samt Användning av bärbar dator under resor/utanför kontoret.
Mars	*Intranätsartikel*	Publicera en artikel på temat Social Engineering.
	Grundläggande utbildning: e-utbildning	Kommunicera till alla anställda att den grundläggande e-utbildning genomförs vart tredje år. Säkerställ att alla nyanställda genomfört utbildningen och följ upp redan anställda.
April	*Styrgruppsmöte*	Uppdatering av status samt behov av stöd.
Maj	*Djupgående vidareutbildning*	Brown-bag lunch[18] för Ekonomiavdelningen och Administrativa Ledningsassistenter på temat Informationsöverföring via mejl.
	Nano-Utbildning[19]	Utbildning till alla anställda på temat Spam och Phising. Utbildningen delas upp i fyra mejlutskick.
Juni	*Forum för informationsdelning*	Sammankomst för IT- och informationssäkerhetspersonal
	Test på individnivå	Placera ut lappar på kontoret med en QR-kod och texten ”skanna och få en iPad”. Mät och följ upp resultatet.
	Styrgruppsmöte	Uppdatering av status samt behov av stöd.
Juli	*Intranätsartikel*	Publicera en artikel på temat Lösenords-användning samt skriv kort återkoppling om test på individnivå genomförd i juni.

18 Med brown bag lunch avses informella möten under lättare former över lunch som är såväl resurseffektivt som ett sätt för anställda att socialisera, läs mer https://www.investopedia.com/terms/b/brown-bag-meeting.asp
19 Med Nanoutbildning avses små utbildningsaktiviteter t.ex. via e-post som sprids ut på många tillfällen för att få god effekt på kunskapshöjning, se t.ex.: https://www.junglemap.com/sv/ciso?hsCtaTracking=87ee3125-45ac-4d48-b57c-b329d43e9b58%7Ce589478a-1720-4f83-bfac-12413d29c3a3

Augusti	*Djupgående vidareutbildning*	Webinar med Utvecklare och Systemadministratörer på temat Säker kodning.
September	*Rapportering till styrelsen*	Information till styrelsen om cybersäkerhetsrisker och status på åtgärder.
	Styrgruppsmöte	Uppdatering av status samt behov av stöd.
Oktober	*Cybersäkerhetsvecka*	Separat agenda.
November	*Djupgående vidareutbildning*	Rundabordssamtal med Juridik- och Compliance avdelning på temat Externt styrande regler och föreskrifter
	Nano-Utbildning	Utbildning utskickad till alla anställda på temat Typhändelser. Utbildningen delas upp i fyra mejlsutskick.
December	*Forum för informationsdelning*	Sammankomst för cybersäkerhets-ambassadörer.
	Enkätundersökning	Mät existerande Cyber Awareness-förmåga baserat på förmågematris. Samla in data genom enkät som skickas till alla anställda. Resultatet ligger till grund för nästkommande års Cyber Awareness-arbete.

Verifiering av förmåga

För att validera resultatet av genomförda Cyber Awareness-aktiviteter kan den individuella och organisatoriska förmågan mätas. Verifiering av förmåga kan utföras genom insatser riktade direkt mot den anställda (individuell förmåga), med hjälp av olika test eller genom övergripande analyser av den organisatoriska förmågan (organisatorisk förmåga).

Verifiering av individuell förmåga

Fokusgruppens medlemmar beskriver hur deras organisationer med hjälp av konkreta typhändelser testar den egna personalens förmåga. De beskriver vidare att förmågan på individnivå kan verifieras genom annonserade eller oannonserade tester. Ett oannonserat test är uppbyggt enligt de metoder faktiska angripare använder. Primärt lyfter fokusgruppens medlemmar upp phishing- och social engineering-tester, vilka ger en indikation på individens förmåga och medvetenhet om cyberrisker. Ett konkret exempel som omnämnts vid en av fokusgruppspresentationer är en organisation som placerat upp lappar på kontoret med en QR-kod och texten ”skanna och få en iPad”.

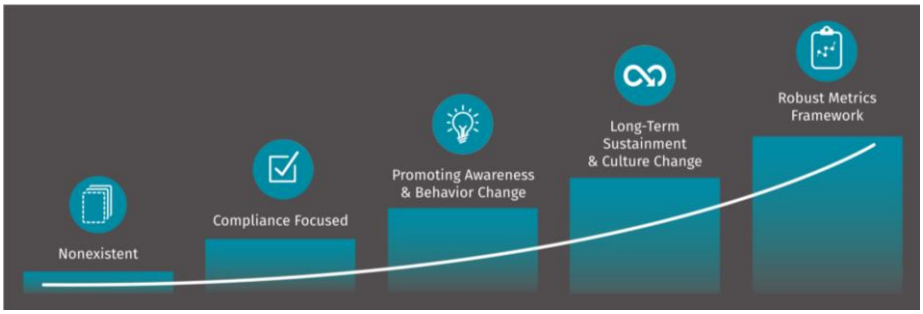
Phisingtester kan systematiskt genomföras kvartalsvis och efter olika teman anpassade efter målgrupp och region. Vid ett särskilt strukturerade phisingtest-program får den testade individen efter phisingmejlet också ett uppföljningsmejl som informerar om

personen agerat i enlighet med organisationens riktlinjer. Upprepade negativa resultat kan även trigga särskilda utbildningsinsatser för personen. Information från dessa tester kan utgöra ett viktigt ingångsvärde för det framtida Cyber Awareness-arbetet.

Verifiering av organisationens förmåga

Tillgänglig litteratur belyser vikten av att verifiera och mäta den organisatoriska förmågan. Fokusgruppens medlemmar lyfter särskilt fram SANS ”Security Cyber Awareness Maturity Model”[20]. SANS modell beskriver fem mognadsnivåer enligt figuren nedan. Genom att använda en mognadstrappa i enlighet med exemplet kan prioriterade åtgärder implementeras baserat på vilken mognadsnivå organisationen har som målbild. Mognadstrappan är således ett verktyg för att definiera nuläge och önskad målbild som grund för den strategiska Cyber Awareness-planeringen.

Som stöd för att verifiera och mäta förmågan tillhandahåller SANS ett Excel dokument för analys[21]. Dokumentet beskriver indikatorer som ansvarig person kan använda i arbetet med Cyber Awareness för att förstå var i mognadsmatrisen organisationen befinner sig. Information att används för analys mot beskrivna indikatorer kan exempelvis utgöras av enkäter, intervjuer och observationer användas.



Figur 7. SANS Security Cyber Awareness Maturity Model.

Även CPMI-IOSCO[22] och NIST belyser att förmåga bör verifieras. NIST föreslår övningar som en verifieringsmetod. Att mäta den organisatoriska förmågan kan således genomföras genom konkreta övningar eller genom mer sofistikerade enkäter och studier.

Istället för den mognadstrappa SANS skapat hänvisar NIST istället till The Kirkpatrik Model[23]. Modellen, som avser mäta resultatet av en utbildnings-/övningsinsats delar, utgörs av följande nivåer:

---

20 https://www.sans.org/security-Cyber Awareness-training/blog/security-Cyber Awareness-maturity-model-kit
21 SANS-SA-SecurityCyber AwarenessMaturityModel-Indicators

[22] *22 CPMI/IOSCO (2016), Guidance on cyber resilience for financial market infrastructures, avsnitt 9.3, sida 22*
18 NIST Special Publication 800-16 Revision 1 (3rd Draft), A Role-Based Model for Federal Information Technology/Cybersecurity Training, (2014), Sid. 51

1) ***Reaction:*** *To what degree participants react favourably to the learning event,*
2) ***Learning:*** *To what degree participants acquire the intended knowledge, skills and attitudes based on their participation in the learning event,*
3) ***Behaviour:*** *To what degree participants apply what they learned during the training when they are back on the job*
4) ***Results:*** *To what degree targeted outcomes occur, as a result of learning event(s) and subsequent reinforcement.*

Beroende på organisationens struktur och arbetssätt bör lämplig mognadsmodell väljas alternativt produceras av och för den egna organisationen.

Förmåga kan även verifieras genom redteamtest. För vidare läsning om redteam tester – se FSPOS PM ”Former och metoder för test av cyberresiliens”[24].

Avslutning

De människor som arbetar i och för en organisation är en nyckelfaktor för en god förmåga att hantera cyberrisker. Organisationer bör därför arbeta strategiskt och långsiktigt med att höja individernas kunskap genom ett systematiskt och strukturerat Cyber Awareness arbete. Arbetet bör vara förankrat på högsta nivå i organisationen och nå ut till alla anställda genom olika målgruppsanpassade metoder så att organisationens förmåga att hantera cyberrisker kan upprätthållas på en hög nivå.

19 http://www.fspos.se/siteassets/fspos/rapporter/2018/former-och-metoder-for-test-av-cyberresiliens.pdf