Den 30.6.2021

News nr. 11-2021 fra A2012

Til bestyrelsesmedlemmer i antenneforeninger, der er medlem af A2012

1. ”Cybertruslen mod Danmark er meget høj”

Det sagde forsvarsminister Trine Bramsen (S) i en pressemeddelelse den 24.6.2021, hvor hun fortsatte: ”Hver eneste dag bliver vores myndigheder, virksomheder og borgere udsat for angreb eller forsøg på angreb. Det har store konsekvenser for Danmark. Både for vores sikkerhed og demokrati - og for vores økonomi.”

Derfor har partierne bag forsvarsforliget 2018-2023, det vil sige Socialdemokratiet, Venstre, Dansk Folkeparti, Radikale, Konservative og Liberal Alliance indgået en ny aftale, der tilfører bekæmpelsen af cybertrusler nye 500 mio. kr.

Pengene skal blandt andet bruges til øget monitorering, som skal opfange og varsle om cyberangreb rettet mod samfundskritiske virksomheder, samt et cyberindsatshold, der kan rykke ud og hjælpe virksomheder og myndigheder, som er blevet ramt af hackerangreb. A2012 anser aftalen for god og nødvendig efter et år, hvor både Danmark og resten af verden er blevet ramt af omfattende hackergreb.

2. A2012 er aktiv og giver gode råd om cybersikkerhed

I A2012 kikker vi jævnligt på overvågningen af vores egen hjemmeside, der dagligt viser masser af forsøg på indtrængen fra mange forskellige lande.

I januar 2020 havde A2012 sagen oppe på repræsentantskabsmødet, hvor senior IT-specialist Keld Norman, Dubex A/S, holdt et særdeles inspirerende oplæg om emnet, der efter selve repræsentantskabsmødet blev suppleret med orientering om ”det mørke internet”, Tor-nettet m.v. Mødedeltagere fik adgang til Keld Normans PPT-præsentation på 610 MB.

Efter mødet har FU udarbejdet en grundig vejledning, der er til rådighed for alle bestyrelsesmedlemmer i A2012’s medlemsforeninger. Den blev førstebehandlet på repræsentantskabsmødet i oktober 2020 og vedhæftes dette News i pdf-format som **GODE RÅD OM CYBERSIKKERHED, 2. udgave, juni 2021**.

Hvis du vil forbedre din egen og din forenings cybersikkerhed anbefaler FU, at du sætter tid af til hen over sommeren til at studere og arbejde med de gode råd. Tag det også op på næste bestyrelsesmøde.

Disse råd og de 3 artikler nedenfor kan også bruges til foreningernes hjemmesider og nyhedsbreve.

3. Bedre cybersikkerhed vores lokalnetværk

Start med at forhøre dig om, hvorledes du får adgang til indstillinger i dit modem hos din forenings tekniske assistance eller eventuelt hos din internetudbyder, dersom du ikke allerede ved, hvorledes adgang til dit modem/router etableres.

Takket være trådløst lokalnetværk (WLAN) findes kabler næsten kun hos hverdagens brugere med høje ydelseskrav. Det trådløse netværk er meget udbredt til forbindelser til bærbare computere, smartphones, kameraer og overvågningsudstyr til f.eks. køleskabe mv.

WiFi-enheder forbinder sig til routeren og dermed til internettet. Det rummer også farer. For når det trådløse netværk er blevet brudt, får hackere ofte adgang til et stort antal forskellige enhedstyper, som ikke alle er lige sikre. Det gør det endnu vigtigere at beskytte det trådløse hjemmenetværk.

Her er et par gode tips til højere WLAN-sikkerhed.

For at få en sikker adgangskode skal du bruge mindst 20 tegn og aldrig bruge rigtige ord eller talrække såsom din fødselsdato. De er for lette at gætte.

Det er bedst at skifte mellem tilfældige store og små bogstaver samt tal og specialtegn.

For at du ikke glemmer adgangskoden, kan du bruge en husketeknik, som en bro til at forkorte den til en adgangskode. Fra "Hver aften kl. 18.30 laver jeg to og en halv rulle med smør, flødeost og urter - lækkert!" bliver som "Jkl18: 30Prod2,5RSmØ,FLOUR-I!". Det lyder fjollet, men det hjælper.

Hvis dit WLAN stadig er beskyttet med den fabriksindstillede adgangskode, skal du ændre den; fordi koden normalt står på undersiden af enheden og let kan læses og aflæses af andre måske uvedkommende personer. Nogle producenter bruger endda en identisk adgangskode til alle deres netværksenheder!

Det er bedst at give besøgende adgang til internettet via gæstenetværket, som er adskilt fra det almindelige netværk.

WLAN-adgangskoden kan oftest ændres via adgangen til din router. Indtast http://routerens adresse i din browser, og log ind med routerens adgangskode. Klik på WiFi og sikkerhed i menuen, hvorefter adgangskoden kan ændres og kryptering sættes. Husk at bekræfter ændringen, så den træder i kraft.

4. WiFi-kryptering

Hvis WLAN-krypteringsmetoden ikke er god, er selv den bedste adgangskode ikke længere en holdbar sikkerhed. Netværksenheder bruger typisk WPA-, WPA2- og WPA3-metoder. For at krypteringen kan finde sted, skal både netværksenheden og slutenheden mestre processen.

Meget gamle enheder bruger kun WPA-metoden. Den betragtes i dag som usikker. Brug derfor WPA2 eller (hvis muligt) WPA3. Sandsynligheden for, at en af dine slutenheder kun understøtter WPA, er meget lav nu om dage. Hvis det alligevel er tilfældet, er det en god grund til, at det er klogt ikke at oprette forbindelse til internettet på disse enheder. På grund af dens relativt høje alder vil det sandsynligvis ikke længere modtage opdateringer og derfor udgør de en sikkerhedsrisiko. Der er enheder, som kan bruge både WPA og WPA2 – altså begge metoder til forbindelser. Brug ikke det og vælg i disse tilfælde en "ren" WPA2.

Næsten alle routere og slutenheder, der i øjeblikket er tilgængelige, bruger WPA2-metoden. Den anses for at være relativt sikker, men kan patches med opdateringer, fordi nogle sikkerhedshuller som "Kr00k" gav hackere adgang tidligere.

WPA3 er den nyeste og mest sikre krypteringsmetode til WLAN. Da ikke alle slutenheder kan håndtere processen, anbefales det at bruge indstillingen "WPA2 / WPA3" i routeren (hvis den er tilgængelig).

For at administrere dette, skal man vide, hvordan man kan få adgang til indstillinger i sin modem/router. Hør hos din forenings tekniske assistance eller hos internetudbyder, dersom du ikke allerede ved hvorledes adgang til din router etableres.

5. Fishing – CEO Fraud – også i antenneforeninger - pas på!

CEO Fraud, også kaldet fishing, er en forholdsvis ny form for kriminalitet. Den består i, at kriminelle sender tilsyneladende ægte mails fra en CEO (direktør, formand) til et firmas økonomifunktion (kasserer), med ordre til at overføre et større beløb straks til en konto, som den kriminelle har adgang til, og hvorfra han kan hæve beløbet.

Det kan også ske for en antenneforening. Vi viser nedenfor en falsk, men ægte udseende mail fra en antenneforeningsformand til en kasserer. Formanden kendte intet til mailen, og kassereren troede, at den falske mail fra formanden var ægte. Nedenstående korrespondance er ægte og A2012 bekendt, men de rigtige navne er ændret:

Denne mail dukker op i kassererens indbakke:

Fra: "Jens Hansen" < formand@lillenet.dk > (formanden)

Sendt: 16. april 2020 12:20

Til: "Søren@lillenet .dk " <kasserer@lillenet.dk> (kassereren)

Emne: Anmodning til april

Hej Søren

Er du tilgængelig nu?

Jeg har brug for, at du overfører EUR 4.620,00 til en modtager i Tyskland i dag. Jeg har bankoplysningerne. Kan betaling foretages nu?

Med venlig hilsen

Jens

Kassereren fatter ikke, at det er bedrageri, og svarer naivt til den, han tror er formanden, men som er den kriminelle:

Sent: 16. april 2020 15:29

Fra: "Søren Jensen" <kasserer@lillenet.dk>

Til: "Jens Hansen" <formand@lillenet.dk>

Emne: re: Anmodning til april

Hej Jens

Betaling til udlandet har jeg privat foretaget mange gange, har du faktura og betalingsoplysninger, så fikser jeg det.

MVH

Søren

Den rigtige formand sender og modtager intet, selv om hans e-mail-adresse er korrekt.

Kassereren modtager dette mailsvar, som han tror er fra formanden, men som er fra den kriminelle:

Fra: "Jens Hansen" < formand@lillenet.dk >

Sendt: 16. april 2020 17:31

Til: "Søren Jensen" <kasserer@lillenet.dk>

Emne: re: Anmodning til april

Hej igen Søren

Her er modtageroplysningerne nedenfor: Foretag en overførsel på 4.620,00 EUR;

Jeg sender dig en kopi af fakturaen, så snart jeg har den til dokumentation.

Bank navn: Postbank

IBAN: DE52 1001 0010 0290 1811 30

BIC (Swift) Kode: PBNKDEFF

Bankadresse: Bahnhof Mainfranken Rosenheim Bayern Muenchen.

Modtagers navn: Kingsley Esechie.

Modtagers adresse: Fasanenstrasse Lanstrasse 86 10623 Berlin.

Beløb: 4,620.00 EUR

Betalingstype: Express

Meddelelse til modtageren: P-F Antenneforening (Purehase)

Betalingsomkostninger: Betalere og modtagere deler.

Sende mig en kopi af betalingskvitteringen, hvornår det er gjort.

/Jens

Kassereren svarer noget naivt:

Sendt: 16. april 2020 18:05

Fra: "Søren Jensen" <kasserer@lillenet.dk>

Til: "Jens Hansen" <formand@lillenet.dk>

Emne: re: Anmodning til april

Det fikser jeg, men hvad har vi købt i det store udland?

MVH

Søren

re: Anmodning til april

to 16-04-2020 18:06

Fra: "Jens Hansen" <formand@lillenet.dk>

Til: "Søren@lillenet.dk" <kasserer@lillenet.dk>

Hej Søren

Betalingen er for den samlede organisationsudvikling og andre logistiktjenester. Jeg sender dig en kopi af fakturaen, så snart jeg har den senere i dag.

Mvh

Jens

Herefter sker er ikke mere. Det vides ikke, hvorfor den kriminelle stoppede. En nærmere undersøgelse afslørede, at de falske mails var sendt fra en hacket konto hos en anden antenneforening.

Desværre holder kassereren sagen for sig selv og fremlagde den først 4 måneder senere i bestyrelsen med en bebrejdende forespørgsel til formanden om, hvad han har haft gang i. Det er naturligvis en tåbelig fremgangsmåde.

Hvis der opstår mistanke om hacking eller andre former for kriminalitet, skal en kasserer eller andre naturligvis omgående sikre sig, personligt eller pr. telefon, hvem der står bagved mystiske transaktioner eller forsøg herpå, og naturligvis også straks orientere både formanden og resten af bestyrelsen.

Med venlig hilsen

***Bernt Freiberg**, formand* bf@a2012.dk, *44402012-1*

***Poul Juul**, næstformand* pj@a2012.dk, *44402012-2*

***Tage Lauritsen**, sekretær* tl@a2012.dk, *44402012-3*

***Carsten Pedersen**, FU-medl.* cp@a2012.dk, *44402012-4*

Kontakt til A2012: Send til FU: fu@a2012.dk