Rammeaftale

Om IT-Sikkerhedsanalyser til DANVA -medlemmer

Vandselskaber er lige som alle andre brancher sårbare over for IT-kriminalitet. Både i Tyskland og i Sverige meldes omfanget af hackerangreb mod bl.a. forsynings-virksomheder at være vokset markant de seneste år. For at hjælpe foreningens medlemmer med at opretholde højest mulige sikkerhed mod cyberangreb og andre trusler, har DANVA indgået en rammeaftale om IT-sikkerhedsanalyser med NetDesign.

Rammeaftalen giver DANVAs medlemmer mulighed for at købe en grundpakke med sikkerhedsanalyse, der er skræddersyet til vandselskaber, til en konkurrencedygtig pris. Derudover kan det enkelte selskab vælge at tilkøbe en række forskellige tillægspakker efter behov.

Det er DANVAs netværk for IT-sikkerhed, der har forhandlet og tilpasset den nye sikkerhedsanalysepakke i samarbejde med NetDesign.

”Vandforsyningerne er at betragte som ”kritisk infrastruktur” og har stor samfundsmæssig betydning. Derfor er det vigtigt, at vi i en tid med stigende digitalisering har fokus på informations-sikkerhed. I netværket har vi vurderet, at den nye sikkerhedsanalysepakke er et godt tilbud og et overskueligt værktøj, som kan hjælpe vandselskaberne til at få et overblik over status på deres informationssikkerhed og dermed mulighed for at igangsætte passende aktiviteter,” siger Finn Asmussen, chefkonsulent i IT-afdelingen hos HOFOR og tovholder i DANVAs netværk for IT-sikkerhed.

Indblik og operationelle anbefalinger

Den nye sikkerhedsanalyse-grundpakke er testet i Syddjurs Spildevand, hvor IT-ansvarlig Martin Damgaard er godt tilfreds med udbyttet af analysen.

”Sikkerhedsanalyse-grundpakken vil passe godt til langt de fleste DANVA-medlemmer. Den giver et godt indblik i, hvordan sikkerhedsberedskabet fungerer i praksis, og slutrapporten giver fornuftige og operationelle anbefalinger til, hvordan man bedst kan forbedre det eksisterende sikkerhedsberedskab,” siger han.

Indholdet i grundpakken er sammensat ud fra, at de fleste vandselskabers sikkerheds-beredskab i store træk er sammenlignelige, og at der er mange lighedspunkter i de udfordringer, de står overfor. Målet er at belyse, hvilke indsatser, der giver størst værdi for det enkelte vandselskab.

”I virkeligheden handler det ikke om at bruge mange penge på nye, store sikkerhedsløsninger, men i højere grad om at vide præcis, hvilke systemer og data, der bør beskyttes, og hvordan det gøres mest effektivt og økonomisk,” siger Ronnie Abrahamsen, sikkerhedsekspert i NetDesign.

360° SIKKERHEDSANALYSE FOR VANDFORSYNINGER

Grundpakken består af:

- Sikkerheds-modenhedsanalyse
- Netværkstrafik-analyse
- Sårbarhedsskanninger - internt og eksternt
- Intern Penetrationstest
- Workshop
- 360° Sikkerhedsanalyse-rapport

Eksempler på tillægspakker:

- Basis OT-Sikkerhedsanalyse
- Advanced OT-Sikkerhedsanalyse
- Ekstern Penetrationstest
- Webapplikationstest
- Fysisk Penetrationstest
- Phishing sårbarhedsanalyse

Prisen for 360° Sikkerhedsanalyse for vandforsyninger, grundpakken, er 18.750,- kr.

Tilvalg af tillægspakker m.m. aftales og prissættes i samarbejde med den enkelte forsyning.

Kontakt NetDesigns sikkerhedseksperter for yderligere information om indhold, beskrivelser og hvordan I kommer i gang:

Ronnie Abrahamsen, mobil 2929 1010, roab@tdc.dk
Bo Hermansen, mobil 2234 5265, boh@tdc.dk

INDHOLD
SIKKERHEDSANALYSE GRUNDPAKKE

1. Sikkerheds- Modenhedsanalyse

På baggrund af tekniske analyser, interviews og dataindsamling, udarbejdes en vurdering af jeres sikkerheds-modenhed på følgende parametre:

- Design og funktionalitet af den samlede Sikkerhedsløsning
- Forankring af sikkerhedspolitikker og -processer i det daglige Sikkerhedsarbejde
- Evnen til at forhindre, opdage og bekæmpe angreb
- Processer omkring retablering af betroet tilstand og efterfølgende analyse og konsekvens rapportering

2. Netværks-Trafikanalyse

Al erfaring viser, at der i de fleste virksomheder allerede findes skadelig eller uønsket trafik inde på netværket. Vi undersøger i hvilket omfang, det er tilfældet for jer, ved at analysere trafikken inde på jeres netværk.

Der opsættes en passiv enhed inde på netværket, som i en periode på typisk en uge, opsamler og analyserer netværkstrafikken. Efterfølgende vil resultaterne blive præsenteret sammen med anbefalinger til, hvordan uønsket trafik fjernes.

3. Sårbarhedsskanninger (Ekstern + Intern)

En vigtig disciplin i håndtering af de trusler I står overfor, er at få et overblik over de kendte sårbarheder, der findes i jeres infrastruktur. Mange hackerangreb initieres nemlig via en eller flere af disse allerede kendte sårbarheder.

Overblikket skabes gennem målrettede skanninger for sårbarheder både fra Internet siden, og inde fra jeres interne netværk. I får et detaljeret overblik over de sårbarheder som findes, deres betydning og ikke mindst anbefalinger til, hvordan de udbedres.

4. Intern Penetrationstest

Efter sårbarhedsskanningerne ovenfor er udført vil vi arbejde os dybere ned og teste hvordan jeres forsvar fungerer mod angreb, der har penetreret jeres ydre forsvar og således allerede er inde på det interne netværk. Kan angrebet sprede sig til andre og kritiske dele af netværket? Kan en angriber eskalere sine rettigheder til administrator eller kan andre sensitive data eller systemer kompromitteres?

5. Workshop

Resultaterne fra analyserne bliver sendt til jer og gennemgået på en workshop med jeres sikkerheds-team.
Her vil i få mulighed for få uddybet og valideret resultaterne fra analysen inden den endelige rapport udarbejdes.

6. 360° Sikkerhedsanalyse Rapport

Efterfølgende vil NetDesign samle resultaterne i en overskuelig rapport med håndgribelige og operationelle anbefalinger, sammen med en køreplan for implementering af de initiativer, der kan forbedre sikkerheden for jeres forsyningsvirksomhed.
Med rapporten kan i hjælpe forsyningsvirksomheden med yderligere fokusering og optimering af den samlede sikkerhedsløsning.

Pris for DANVAs medlemmer: Kr. 18.750,-

BESKRIVELSE AF
SIKKERHEDSANALYSE TILLÆGSPAKKER – del 1.

Til de medlemmer der, ud over analyserne i Sikkerhedsanalyserne i grundpakken, ønsker en lidt dybere analyse på udvalgte områder tilbydes NetDesign vi en række tillægspakker.
Tillægspakkerne er supplement til grundpakken og de kan ikke tilvælges uden denne.

Ekstern Penetrations test

De fleste hackerangreb bliver stadig initieret og udført udefra, og derfor er de systemer som først bliver ramt, de Internetvendte systemer. I denne test fokuseres der på, i hvilket omfang det er muligt at kompromittere udvalgte systemer, af en udefra kommende angriber og om det ville være muligt, at arbejde sig dybere ind i de bagvedliggende systemer.
Indeholdt er 2 dages test, Pris: Kr. 12.495,-

Test af fysisk sikkerhed

Et væsentligt, men ofte overset element, når vores sikkerhed skal vurderes, er den fysiske sikkerhed. NetDesign vil derfor udføre en test af den fysiske sikkerhed og vil bl.a. forsøge at skaffe sig adgang til udvalgte ubemandede eller bemandede anlæg og/eller andre centrale enheder, med det formål at undersøge om angribere ville kunne placere udstyr som kan ændre måleværdier eller på andre måder kompromittere sikkerheden lignende f.eks. om der kan placeres keyloggere på computere eller servere.
Indeholdt er 2 dages test, Pris: Kr. 12.495,-

SCADA Penetrationstest

Da vores SCADA enheder er helt centrale for vores ydelser, har vi valgt at medtage en speciel test, hvor der udelukkende fokuseres om det er muligt at tilgå centrale SCADA enheder. Testen udføres indefra områder i vores infrastruktur, hvor det under normale omstændigheder ikke burde være muligt at nå enhederne. Men ville en hacker kunne nå kritiske enheder eller systemer på produktionsnetværket?
Indeholdt er 2 dages test, Pris: Kr. 12.995,-

Phishing Sårbarhedsanalyse

Phishing mail fortsætter også i 2019 med at være den primære angrebsvektor for stor set alle cyberangreb og desværre viser alle statistikker at medarbejderne stadig er sårbare overfor disse angreb. Denne Phishing Sårbarhedsanalysen vil undersøge om det er muligt gennem en phishing mail og/eller gennem telefonopkald at franarre login oplysninger som brugernavn og password til jeres netværk, som potentielt ville kunne bruges til at kompromittere jer yderligere.
Indeholdt er analyse af op til 250 medarbejdere, Pris: Kr. 6.995,-

Sikkerhed Awareness Workshop

Vi har sammen med NetDesign sammensat en Workshop hvor vi vil træne og undervise deltagere i at genkende og forholde sig til de fælder og farer der lurer i den digitale verden og forstå hvordan hackere arbejder.
Et gennemgående element vil være at belyse de teknikker og metoder en hacker benytte til at kompromittere IT og OT systemer, samt at træne i roller og reaktionsmønstre under et hackerangreb.
Workshoppen gennemføres på centrale lokationer i landet og gennemføres i hold på ca. 20 medarbejdere.
Indeholdt er 3-4 timers workshop, Pris pr. deltager: Kr. 1.995,-

BESKRIVELSE AF SIKKERHEDSANALYSE TILLÆGSPAKKER – del 2.

Sikkerhedsanalyser af OT-infrastruktur

Cybertruslen imod produktionssystemer, arkitektur og de anvendte kommunikationsprotokoller, som også er defineret som OT-teknologier, er ligesom det generelle trusselniveau på IT systemer stærkt stigende.

NIS-lovgivningen, som fokuserer på sikkerheden omkring samfundets "kritiske infrastruktur", krævet at man har et passende sikkerhedsniveau, så derfor er det afgørende at produktionsinfrastrukturen også indgår i Sikkerhedsanalysen.

OT-infrastrukturen er anderledes end den traditionelle IT-anvendelse på forretningssiden. At gennemføre en sikkerhedsanalyse og efterfølgende komme med anbefalinger til sikkerhedsmæssige forbedringer i forhold til fundne risici kræver en anden indsigt og tilgang ind "forretnings-IT". Derfor har NetDesign valgt at arbejde sammen med SecuriOT, som kan supplere med OT-sikkerheds-ekspertise. SecuriOT udspringer fra Novotek, som i over 30 år har leveret automationssystemer, såsom f.eks. GE iFIX, PTC kepware, etc. til en lang række forsynings- og produktionsvirksomheder.

SecuriOT supplerer NetDesign Sikkerhedspakke med 2 tillægspakker, som netop har fokus på sikkerheden omkring jeres OT-infrastruktur, nemlig Basis OT-Sikkerhedsanalyse og Advanced OT-Sikkerhedsanalyse PLUS

Basis OT- Sikkerhedsanalyse

Den analyse har primært fokus på, hvordan forsyningsvirksomheden arbejder med OT-sikkerhedsmæssige discipliner i dagligdagen. For at kunne analysere "modenheden" omkring OT-sikkerhed, vil tillægsydelsen også tilføje supplerende spørgsmål til "Sikkerheds-Modenhedsanalyse fra grundpakken.
De spørgsmål har fokus på de sikkerhedsmæssige opgaver, som vedrører OT-infrastrukturen og processer i forhold til OT.

Når denne tillægspakke vælges, opnår forsyningsvirksomheden:

- Vurdering af jeres sikkerheds-modenhed på i forhold til OT miljøet
- Anbefalinger til evt. procesmæssige ændringer i "sikkerhedsarbejdet" omkring OT-sikkerhed.

Indeholdt er supplerende spørgsmål samt deltagelse på Workshops, Pris: Kr. 6.995,-

Advanced OT- Sikkerhedsanalyse

Denne sikkerhedsanalyse er en af mere teknisk karakter indeholdende en teknisk vurdering af arkitektur og sårbarheder, som forsyningsvirksomhed er sårbar overfor på OT-infrastrukturen.

Denne analyse kræver en implementering af en passiv enhed, som sættes central i forsyningsvirksomhedens infrastruktur.
Denne enhed skal "sidde" imellem PLC/RTU'er og SRO/SCADA service på en SPAN port.
Det er en udsætning at mindst én enhed implementeres, og at den er i stand til at dække forsyningsvirksomhedens infrastruktur.
Hvis der behov for yderligere enheder til at dække infrastrukturen, så kan dette implementeres fra regning.

Advanced OT-Sikkerhedsanalysen indeholder følgende 3 punkter:

- Kortlægning af aktive enheder på OT-infrastrukturen (f.eks. RTU, PLC, Switche og servere, etc.)
- Kortlægning af forbindelser og trafikmønstre i OT-infrastrukturen (protokoller og trafikmængder)
- Identifikation af evt. kendte sårbarheder på de identificerede komponenter i OT-infrastrukturen.

Når denne tillægspakke vælges, opnår forsyningsvirksomheden:

- Rapportering om infrastrukturen ift. aktive komponenter, forbindelser og trafikmønstre.
- Beskrivelse af Top 5 sårbarheder inkl. anbefalinger til at mitigere disse sårbarheder.
- Anbefalinger til evt ændringer i tekniske setup og arkitektur

Indeholdt er opsætning og nedtagning af passiv enhed, samt deltagelse på Workshops, Pris: Kr. 12.495,-