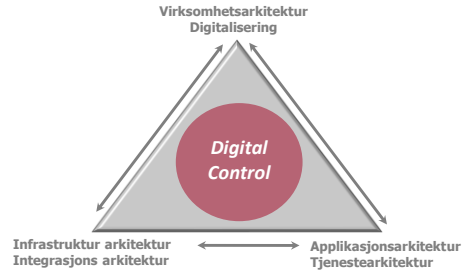
1

Digital virksomhet krever Digital Control



2

Agenda

- Hvorfor arbeide strukturert med en Sikkerhets og sonemodell
- Hvordan implementere et moderne Sikkerhets og sonedesign
- Hvordan passer det inn i sikkerhetsarbeidet overordnet og teknisk

PEDAB

3

Noen angrepsflater og utfordringer

4

Eksempel på sårbarheter – Microsoft basis

Fra: NorCERT [mailto:norcert@cert.no]
Sendt: Tuesday, January 9, 2018 7:44 PM
Til: varselmottakere@cert.no
Microsoft Patche-tirsdag **9. Januar 2018**
Oppsummering:

Microsoft har offentliggjort sine månedlige sikkerhetsoppdateringer i kveld [1]. Det er totalt 61 bulletiner, hvor 17 er vurdert som kritiske.

Denne månedens **patchetirsdag inneholder som vanlig kritiske sårbarheter i Microsoft** sine nettlesere. Spesielt Microsoft Edge. Disse sårbarhetene kan potensielt benyttes til ekstern eksekvering av vilkårlig kode, men **dette forutsetter at brukeren selv aktiverer det skadelige innholdet.**

Det har også blitt sluppet en **kritisk oppdatering til Microsoft Office**(CVE-2018-0797). Denne oppdateringen adresserer en sårbarhet i RTF- parseren til **Microsoft Word**. Dette kan potensielt utnyttes av en angriper til å sende **et spesielt utformet Word-dokument som vil eksekvere vilkårlig kode. Brukeren må selv åpne dokumentet for at angrepet skal lykkes**. Dette angrepet har enda ikke blitt observert benyttet.

5

Eksempel på sårbarheter - infrastruktur

-----Opprinnelig melding-----
Fra: NorCERT <norcert@cert.no>
Sendt: onsdag 15. januar 2020 13:17
Til: varselmottakere@cert.no
Emne: [NorCERT#20855775] [TLP:GRØNN][NCSC-varsel] Oppdatering til Citrix-sårbarhet CVE-2019-19781

De siste dagene har flere norske virksomheter rapportert om vellykkede utnyttelser av sårbarheten. Dette er trolig en konsekvens av at utnyttelseskode for sårbarheten ble publisert 10. januar. NCSC forventer at bruk av denne koden både vil være automatisert og manuelt utført av ulike aktører.

Åpne kilder beskriver hvordan sårbarheten kan benyttes for å blant annet installere bakdører [2] hvor det i noen av tilfellene er gjort med den hensikt å utvinne crypto-valuta. Indikatorer fra noen av forsøkene er beskrevet her [3].

NCSC har per i dag varslet over 470 norske virksomheter om at de er sårbare for utnyttelsen. Dette har utgjort over 1050 unike IP-adresser, og det oppfordres på det sterkeste å mitigere sårbarhetens slik Citrix beskriver [4] frem til en sikkerhetsoppdatering foreligger. Det finnes også en sjekkliste for mitigering som NCSC anbefaler å benytte [5]. Det antas at Citrix publiserer oppdateringen 20. januar for Citrix ADC versjon 11, 12 og 13, mens versjon 10 ser ut til å måtte vente til 31. januar. NCSC antar at norske virksomheter som fortsatt er sårbare må kunne forvente en økning i forsøk på utnyttelse før oppdateringen er sluppet.

The Cybersecurity and Infrastructure Security Agency (CISA) i USA har publisert et verktøy som lar deg selv sjekke om virksomheten er sårbar [6][7]. NCSC anbefaler å benytte seg av dette verktøyet dersom virksomheten ikke har andre metoder for å verifisere om sårbarheten er mitigert eller ikke.

Citrix-sårbarheten CVE-2019-19781 har blitt observert aktivt utnyttet i **Norge og per dags dato foreligger det ikke en sikkerhetsoppdatering.**

NCSC-pulsen vil på bakgrunn av denne ukens komplekse sårbarhetsbilde og påfølgende sikkerhetsoppdateringer derfor bli satt opp til nivå tre (3). **Dette betyr at NCSC vurderer at det er en fare for vellykkede angrep mot digital infrastruktur i Norge.**

6

Topp 25 CWE

1200 - Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors

- Improper Restriction of Operations within the Bounds of a Memory Buffer - *(119)*
- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - *(79)*
- Improper Input Validation - *(20)*
- Information Exposure - *(200)*
- Out-of-bounds Read - *(125)*
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - *(89)*
- Use After Free - *(416)*
- Integer Overflow or Wraparound - *(190)*
- Cross-Site Request Forgery (CSRF) - *(352)*
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - *(22)*
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - *(78)*
- Out-of-bounds Write - *(787)*
- Improper Authentication - *(287)*
- NULL Pointer Dereference - *(476)*
- Incorrect Permission Assignment for Critical Resource - *(732)*
- Unrestricted Upload of File with Dangerous Type - *(434)*
- Improper Restriction of XML External Entity Reference - *(611)*
- Improper Control of Generation of Code ('Code Injection') - *(94)*
- Use of Hard-coded Credentials - *(798)*
- Uncontrolled Resource Consumption - *(400)*
- Missing Release of Resource after Effective Lifetime - *(772)*
- Untrusted Search Path - *(426)*
- Deserialization of Untrusted Data - *(502)*
- Improper Privilege Management - *(269)*
- Improper Certificate Validation - *(295)*

Move to stay ahead

7

Noen sikkerhetsmekanismer

- Next Genration Firewall, Application Firewall
- Proxy løsninger
- Mikrosegmentering og Virtualisering
- IAM og PAM Løsninger
- Antivirus, IPS, IDP
- DLP, Mailsikringsfunksjoner og Antispam
- Filsluser, Robotteknologi, SFTP
- SD-Wan, VPN, NAC
- Cloud overvåkning og kontrollmekanismer
- Backup, Arkivering og Disaster Recovery
- Klientsikring, VDI og Tynnklienter
- Logkorrolering, SIEM og SOC tjenester

8

Tradisjonell sonedeling - Historisk

FIGUR 1: Sikkerhetsarkitektur. Inndeling i soner

Virksomhetens sikkerhetsarkitektur skal ivareta følgende:

- Sensitive personopplysninger skal behandles og lagres i sikrede soner som kun autoriserte brukere har tilgang til. En virksomhet kan opprette flere sikrede soner avhengig av behov.
- Skillet mellom sikret sone og intern sone skal være slik at det ikke er mulig for brukere å overstyre oppsatte begrensninger. Som et minimum må det være én teknisk sikkerhetsbarriere mellom sikret sone og intern sone.
- Skillet mellom eksterne nettverk og sikret sone skal ivaretas av to uavhengige tekniske sikkerhetsbarrierer.
- Ingen tjenester skal kunne initieres fra andre soner og inn i sikret sone. Kun autoriserte tjenester skal kunne initieres utenfra med særskilte tekniske sikkerhetstiltak.
- Ingen nettverkskomponenter, utstyr, databaser eller lignede skal kunne omgå oppsatte sikkerhetsbarrierer, for eksempel at utstyr brukes som fellesløsning for både sikret og intern sone.

Datatilsynets veileder

Move to stay ahead

9

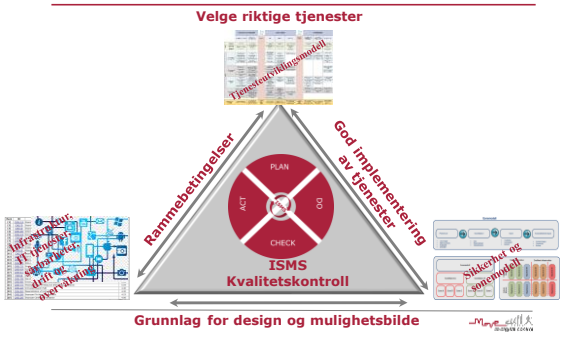
Problemer oppstår..

- Mobilitet blir en naturlig del av arbeidet
- Én ansatt – én PC – én brukerkonto
- Data endrer sensitivitet i faser
- Integrasjon mot eksterne tjenester
- Digitalisering krever at vi *tilbyr* tjenester til eksterne aktører
- De samme systemene benyttes for sensitiv og ikke-sensitiv informasjonsbehandlig
- Virtualisering fjerner fysiske skiller
- Administrasjon krever utvidet tilgang til alle deler av nettverket

Move to stay ahead

10

Virksomhetsforankret digitaliserings og sikkerhetsmodell



11

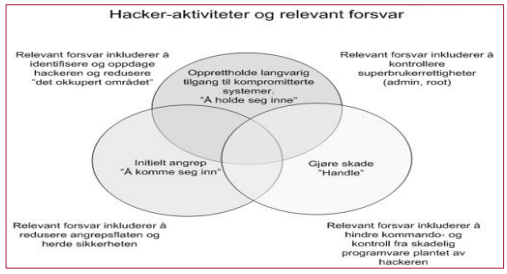
Moderne sonedeling – men hvordan?

- Vektlegge eksponering av tjenestene mer enn system- og informasjonskritikalitet
- Ekskluderer ikke å kunne beskytte og separere systemer ut fra informasjonskritikalitet, men det er sekundært
- Praktisk tilnærming til en 3-lags arkitektur (presentasjon, applikasjon, data)
- En sonemodell med en praktisk tilnærming reduserer kompleksiteten i implementering og dag-til-dag administrasjon av sonemodellen

Move to stay ahead

13

Forsvar i dybden er enest mulige forsvar!



14

Konseptet bak Zero trust

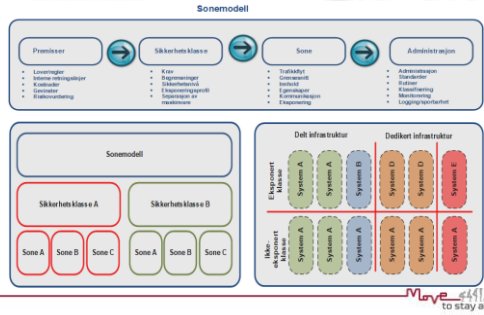
15

Hovedmomenter i modellen

- *Sikkerhetsklassifisering* identifiserer tillitsnivå og beskriver et systems operasjonelle krav og eksponeringsprofil
- *Soneinndeling* sikrer at et systems funksjonelle komponenter er separert og gruppert i henhold til sin natur og kommunikasjonskrav
- *Sikkerhetsmonitorering* for å verifisere tillitsnivået til en sikkerhetssone, og er kritisk for effektiv hendelseshåndtering

16

Moves tilnærming til sonedeling

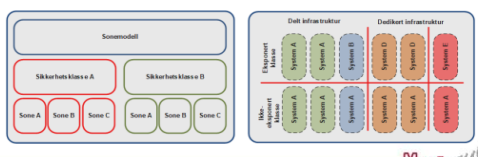


Sikkerhetsklasser

- En sikkerhetsklasse er en paraply for en samling sikkerhetssoner som inneholder systemkomponenter med lik eksponeringsprofil, tillitsnivå og sikkerhetskrav
- En sikkerhetsklasse har eierskap over alle soner innenfor klassen. Et regelsett for en sikkerhetsklasse kan ikke overstyres av regelsett fra en annen sikkerhetsklasse
- Det er ikke noe gitt antall sikkerhetsklasser eller soner

Sikkerhetsklasser

- Kommunikasjon mellom systemer innenfor en sone eller mellom soner kan kontrolleres ved hjelp av aksessregler
- Kommunikasjon mellom sikkerhetsklasser *skal* inspiseres og logges

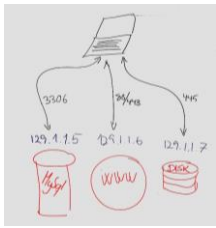


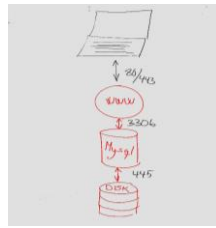
Sikkerhetsklassifisering

- Hvert enkelt system brytes ned (splittes opp) i funksjonelle komponenter, hvor hver komponent (og tilhørende data) plasseres i utvalgte sikkerhetsklasser i henhold til *tillitsnivået*.
- *Tillitsnivået* indikerer sannsynligheten for at et system kan bli kompromittert, eksempelvis som følge av eksponering

20

Sonemodell – tilnærming





21

Separasjon og gruppering

- Enkeltkomponenter i et system kan ha forskjellige eksponeringsprofiler og sikkerhetskrav
- Følger som oftest av spesielle egenskaper eller data de lagrer eller prosesserer
- En gjennomtenkt separasjon og gruppering av systemkomponenter gir viktige bidrag til fremtidige utvidelser
- Digitaliseringsprosesser eller nye brukerbehov, kan implementeres uten å kompromittere sikkerheten

22

Separasjon og gruppering

- Enklere med tjenesteutsetting: Det kan gis tilgang for tredjepart uten å risikere å eksponere systemer som ikke er relevante
- Forenkler prosessen med å gi tilgang til systemer, om det er for sluttbrukere, partnere eller andre systemkomponenter
- Er helt nødvendig for monitorering og effektiv hendelseshåndtering

Move to stay ahead

23

Tillitsnivåer

Tillitsnivået kategoriseres i fire distinkte grupper:

GRØNN indikerer en eksponert klasse med komponenter som kommuniserer med ikke-betrodde parter

ORANGE indikerer en ikke-eksponert klasse med komponenter som primært kommuniserer med andre ikke-eksponerte systemer. Komponenter i denne klassen *kan* også kommunisere direkte med eksterne *betrodde* parter og systemer i GRØNN klasse

RØD indikerer en ikke-eksponert klasse med komponenter som ALDRI MÅ kommunisere direkte med eksterne parter

UKJENT indikerer en systemkomponent utenfor sonemodellen med et utilstrekkelig eller ukjent tillitsnivå.

Move to stay ahead

24

Kriterier for klassifiseringen

GRØNN	
Når	Systemkomponenter som typisk krever direkte kommunikasjon med ikke-betrodde nettverk som eksempelvis Internett eller nettverk hvor tillitsnivået er ukjent, eller komponenter som ikke har behov for sikkerhetsnivået til ikke-eksponerte systemer.
Prinsipp	Komponenten MÅ IKKE lagre interne data Komponenten KAN kommunisere med ikke-betrodde parter Komponenten KAN ha tilgang til interne komponenter Komponenten KAN prosessere interne data
Eksempel	En Internett-eksponert komponent, for eksempel webserver-komponenten av "www.move.no"

ORANGE	
Når	Ikke-eksponerte eller interne systemkomponenter som ikke må eksponeres til ikke-betrodde nettverk eller som ikke har behov for direkte kommunikasjon med slike nettverk.
Prinsipp	Komponenten MÅ IKKE kommunisere direkte med ikke-betrodde parter Komponenten KAN kommunisere direkte med eksterne **betrodde** parter Komponenten KAN inneholde (lagre) interne data
Eksempel	En ikke-eksponert som en fileserver eller databaseserver. Det kan også være applikasjonsservere med tilgang til andre interne systemer.

RØD	
Når	Ikke-eksponerte systemkomponenter som krever et forhøyet nivå av tillit, som for eksempel kritiske administrative systemer (dvs systemer som administrerer infrastruktur som kjernenettverk, samfunnskritisk infrastruktur eller infrastruktur for datasenteret), eller systemer som inneholder personsensitive opplysninger.
Prinsipp	Komponenten MÅ IKKE kommunisere med ikke-betrodde parter Komponenten MÅ IKKE tillate direkte innkommende kommunikasjon fra eksterne betrodde parter Komponenten KAN kommunisere med eksterne **betrodde** parter Komponenten KAN inneholde (lagre) interne data
Eksempel	Kjerneinfrastruktur og tilhørende administrative systemer, filservere og databaseservere som inneholder personsensitiv informasjon.

Move to stay ahead

25

Utdrag fra kravliste

Sikkerhetsklassifisering

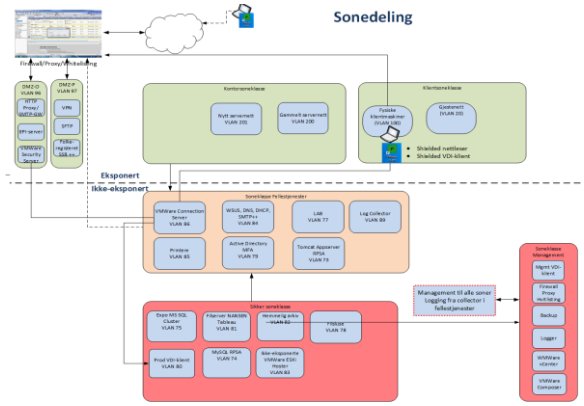
Krav 1	Systemkmponenter i sonemodellen MÅ sikkerhetsklassifiseres i henhold til tillitsnivået (GRØNN, ORANGE, RØD)
Krav 2	Data tilhørende en systemkomponen kan ha betydning for sikkerhetsklassifiseringen
Krav 3	Systemkomponenter MÅ *grupperes* i henhold til sitt tillitsnivå

Separasjon

Krav 4	Systemkomponenter MÅ separeres i henhold til individuelle eksponeringskrav.
Krav 5	Systemkomponenter MÅ separeres i henhold til individuelle kommunikasjonskrav, men KAN grupperes med tilsvarende systemkomponentener som har de samme kommunikasjonsbehovene.
Krav 6	Systemkomponenter MÅ separeres i henhold til individuelle egenskaper
Krav 7	Komponenter fra ett system SKAL normalt separeres fra komponehter tilhørende andre systemer.
Krav 8	Systemkomponenter MÅ IKKE grupperes sammen med andre systemkomponenter med andre egenskaper

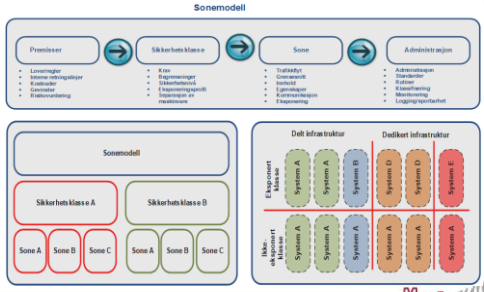
Move to stay ahead

26



27

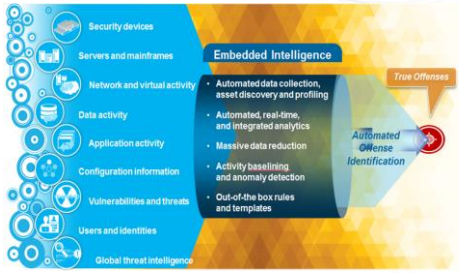
Moves tilnærming til sonedeling



Move to stay ahead

31

Sikkerhetsovervåkning gjennom logkorrelering og baselining

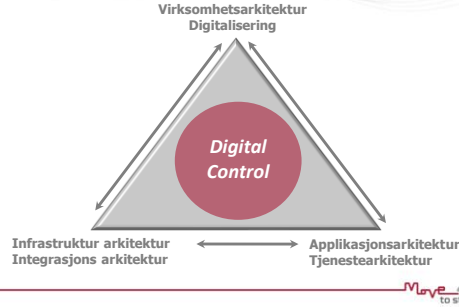


32

Beskytt privilegerte brukerkontoer

33

Digital virksomhet krever Digital Control



34