ezenta
Sikre rammer om IT

SECURE DASHBOARD

Konklusion og anbefalinger for

Systemhuse

METODE

Ezenta har gennemført analyse af otte systemhuse og besøgt fire lægehuse

- De otte systemhuse leverer lægesystemer til PLO's medlemmer.
- Ezenta's resultater er baseret på informationer, som systemhuset har oplyst under interviews og i det omfang, som det viste sig nødvendigt, opfølgning på mails.

Systemhuse

- Alle systemhuse er blevet besøgt
- Rapporten er blevet udarbejdet på baggrund af interview
- Stikprøve er udført
- Sikkerhedstest er gennemført på udvalgte internet vendte systemer
- Relevant dokumentation er gennemlæst hvor der fandtes

Lægehuse

- Gennemført besøg ved 4 klinikker
- Rapporten er blevet udarbejdet på baggrund af interview
- Konklusioner baseret på de 4 klinikker er vurderet i samråd med systemhuse, at de giver ret relativ retvisende billede af sikkerheden ved de enkelte klinikker
- Stikprøve er ikke udført
- Dokumentation er gennemlæst hvor der fandtes
    - Overordnet konklusion på dette område er forbundet med noget usikkerhed

KONKLUSION – SYSTEMHUSE

- De fleste systemhuse er ikke ISO certificeret eller basere deres processer på en anerkendt standard.
- Ingen systemhuse har påtaget sig det fulde sikkerhedsansvar for kunder.
- Sikkerheden bliver i stort omfang svækket baseret på ønsker fra kunder.
  - Her kan særligt nævnes frekvens af ændringer af password og kompleksitet af disse
- De fleste systemhuse tillader at kunden vælger anden leverandør af backup eller ingen backup løsning
- Et par systemhuse har en ad-hoc tilgang til interne processer.
- Systemhusene har en ansvarlig omgang med informationer.
- En række systemhuse benytter underleverandør til deres hosting.

Systemhuse udgør ikke det svageste led i forhold til personhenførbar informationer

KONKLUSION – LÆGEHUSE

Baseret på indsamlede informationer fra 4 lægehuse, er det tvivlsomt om alle PLO's medlemmer på nuværende tidspunkt kan opfylde kravene i forhold til GDPR artikel 32 om "ensure a level of security appropriate to the risk"

Findings:

- Der er en forventning hos de besøgte lægehuse om, at ansvaret for lægehusets IT-sikkerhed ligger ved det enkelte systemhus. Interviews har bekræftet dette. Ezenta har ikke funden grundlag for at dette skulle være tilfældet.
- Flere af lægerne har ikke implementeret de "sikkerhedspakker", som systemhusene tilbyder.

Overordnet anbefalinger:

- Lægerne og klinikpersonalet kunne med fordel blive mere eksplicit oplyst en sikkerhedsminimumsliste i forhold til forsvarlig omgang med personhenførbar informationer.
- Lægerne kan i de fleste tilfælde vælge mellem en hosted eller onsite løsning for opbevaring af patientdata. Der er minimal forskel, ud fra et sikkerhedsmæssigt synspunkt, i løsningerne, men i tilfældet, hvor medlemmerne fravælger sikkerhedspakker, så giver den hostede løsning bedre beskyttelse.

STATISTIK FOR SUNDHEDSSEKTOREN

For sundhedssektoren er de største ydre trusler baseret på ”Verizon breach report 2017”

Top 3 patterns	Privilege Misuse, Miscellaneous Errors and Physical Theft and Loss represent 80% of breaches within Healthcare
Threat actors	32% External, 68% Internal, 6% Partner (breaches)
Actor motives	64% Financial, 23% Fun, 7% Grudge (breaches)
Data compromised	69% Medical, 33% Personal, 4% Payment
Summary	Healthcare has the unenviable task of balancing protection of large amounts of personal and medical data with the need for quick access to practitioners. Internal actors are well represented with employees accessing patient data out of curiosity, or to commit identity fraud.

- Ransomware fortsætter med at være en af de mest fremtrædende trusler.
- Sofistikerede cyberangreb mod europæisk kritisk infrastruktur er en reel trussel, der forekommer angreb ved hjælp af almindeligt tilgængeligt software.
- Utilstrækkelig IT-sikkerhed på enheder koblet på internettet vil resultere i, at følsomme data hvert år bliver ulovligt tilgået. Overvejende sandsynligt, at vi kommer til at se store lækager henover de næste år.

KONKLUSION OPSÆTNING - PLO MEDLEMMER

Væsentlige fund

En del computere har ingen patch management software

Tredje Parts programmer som fx, adobe reader, flash osv, bliver ikke opdateret, i nogle tilfælde skal lægen selv søge for at opdatere, og dermed er sandsynligheden for at ransomware eller malware kan udnytte en kendt sårbarhed relativ stor og sandsynligheden for et nedbrud eller forekomst af infektion er tilstede.

Hardware kan blive indkøbt fra alle steder

Det er i sig selv ikke et sikkerhedsproblem at PLOs medlemmer kan købe hardware valgfrit, men det kan medføre at indkøbte PCer ikke har en sikkerhedsmæssige opsætning, da mange computere som købes enkeltevis er opsat med henblik på at få private kunder i gang så hurtigt som muligt, uden tanke på sikkerhed.

KONKLUSION OPSÆTNING - PLO MEDLEMMER

Væsentlige fund

Backup løsning bliver fravalgt ved visse læger

Et antal medlemmer har fravalgt backup ved systemhusene, og selv om det ikke nødvendigvis betyder at disse står uden backupløsning, så er det uomtvisteligt en dårlig løsning, at nogle medlemmer har valgt backup som usb/harddisk og som tilmed befinder sig i samme skab som serveren. Sandsynligvis bliver disse backup løsninger ikke testet på samme måde som en professional løsning.

Lægerne har en meget dårlig password politik

Både i forhold til password til medlemmernes egen computer og som adgang til systemhusenes software, så benyttes der i mange tilfælde dårligt konstruerede passwords som fx

Brugernavn: xx password: xx12345

Disse passwords bliver ofte aldrig skiftet og bliver dermed brugt i årevis (optil 10 år)

Det betyder at et password er nemt at hacke, men også at det kan benyttes af hackeren i årevis uden at det bliver opdaget.

KONKLUSION OPSÆTNING - PLO MEDLEMMER

Væsentlige fund

Lægens computer bliver benyttet til andre formål

Når lægens computer benyttes til at tilgå internettet og eksempelvis læse e-mails, bliver den enkelte læge i stort omfang udsat for alle de trusler der findes på internettet. Det betyder at sandsynligheden for at en læge får hacket sin computer er relativ stor, når det ses i sammenhold med det sikkerhedsniveau der er på den enkelte computer

Fysiske sikring af serveren er ofte meget ringe

Den fysiske sikring af servere placeret ved lægen er ofte en ulåst dør til et klædeskab. Det betyder at ønsker en ondsindet person at opnå adgang til serveren, vil det ofte være en ukompliceret opgave.

KONKLUSION OPSÆTNING - PLO MEDLEMMER

Væsentlige fund

- Der er ingen formaliseret patch af software eller sikker opsætning af hardware
- Hardware kan frit indkøbes fra elektronikbutikker.
- Backup løsninger bliver fravalgt ved et antal læger (ukendt hvilken anden løsning der benyttes)
- Lægerne benytter efter egen ønske meget svage passwords som sandsynligvis aldrig bliver skiftet
- Ofte blive lægens computer benyttet til andre formål
- Fysik sikring af server er ofte meget ringe

Anbefalinger

- Der bør gennemføres awareness kampagne hos alle PLOs medlemmer, og der kan med fordel blive oplyst en minimumsliste i forhold til forsvarlig omgang med personhenførbar informationer.

DELKONKLUSION– SIKKERHED

Sammenfatning af vores fund indenfor de enkelte områder

- Der er som udgangspunkt ikke medtaget fund som kun gør sig gældende ved et enkelt systemhus.
- De fund som bliver præsenteret i delkonklusionerne er områder eller mangler som gør sig glædende ved de fleste systemhuse.
  - Som eksempelvis certificeringer. Vi skriver at systemhuse kan drage nytte af en formaliseret standard som ISO. Det er naturligvis ikke gældende for systemhuse som har eller er på vej til at blive certificeret.

DELKONKLUSION INFORMATIONSSIKKERHEDSSTYRING

Væsentlige fund

Der benyttes ikke en anerkendt standard

De fleste systemhuse benytter ikke en anerkendt standard i forhold til politikker og processer. Det betyder i flere tilfælde at der ikke er nedskrevne processer og processer som kan være personafhængig. Det vil give et klart overblik og generelt løft for systemhusene hvis man valgte at gå ud fra en anerkendt standard som fx ISO.

Begrænset risikovurdering

Der udføres kun i begrænset omfang formaliseret risikovurdering. Det kan være en naturlig konsekvens af, at der ikke benyttes en fx ISO, og systemhuset kan derfor miste indblik/overblik over de svagheder som findes i virksomheden.

Den fysiske sikring af den enkelte server, som er placeret ved lægen, består ofte af en uløst dør til et klædeskab. Det betyder at ønsker en ondsindet person at opnå adgang til denne server vil det ofte være en ukompliceret opgave.

DELKONKLUSION INFORMATIONSSIKKERHEDSSTYRING

Væsentlige fund

- De fleste systemhuse benytter ikke en anerkendt standard i forhold til deres politikker og processer
- Der udføres kun i begrænset omfang formaliseret risikovurdering

Anbefalinger

- Alle Systemhuse bør vælge at tilrettelægge deres processer efter en anerkendt standard – For IT generelt kan vælges ISO 27001
- Gennemføre en risikovurdering for at kunne målrette systemhusets it-sikkerhedsindsats, en risiko-vurdering kan være baseret på ISO 27005

DELKONKLUSION NETVÆRKSSIKKERHED

Væsentlige fund

Netværket bliver ikke overvåget

De fleste systemhuse har ikke en automatiseret overvågning af logfiler, sagt på en anden måde, der findes ikke et Security Information & Event Management (SIEM) system. Fordelen ved at benytte sig af et SIEM system er, at man kan være på forkant med angreb og hvis et angreb lykkes kan skaden hurtigt minimeres.

Gennemsnittiden for at opdage et angreb på virksomheder uden SIEM er 206 dage.

Ingen NAC løsning

Ganske få systemhuse benytter en Network Access Control (NAC) løsning, hvilket betyder at alle udefrakommende kan tilslutte udstyr på netværket. Det giver også en mulighed for at tilsluttet udstyr kan blive ”glemt” og dermed ikke opdateret. Derfor giver et netværk uden SIEM løsning, statistiske set flere sårbarheder.

DELKONKLUSION NETVÆRKSSIKKERHED

Væsentlige fund

Traditionelle firewalls

Systemhusene benytter traditionelle firewalls som ikke er next generation. Det er firewalls som ikke tilbyder nye features der efterhånden anses som de facto standard. Det betyder at der er en række trusler som i dag anses som kendte der ikke bliver stoppet eller blokeret. De traditionelle firewalls tilbyde ikke en tilstrækkelig beskyttelse i forhold til det aktuelle trusselsbillede

DELKONKLUSION NETVÆRKSSIKKERHED

Væsentlige fund

- Netværket bliver ikke overvåget på en automatiseret måde ved langt de fleste systemhuse.
- Ganske få systemhuse benytter en NAC løsning, for de som ikke har en NAC løsning betyder det, at alle i princippet kan tilslutte udstyr til netværket.
- Systemhusene benytter traditionelle firewalls der ikke tilbyder nye features som efterhånden anses som de facto standard.

Anbefalinger

- Bør etablere en løsning der sikrer at sårbarheder detekteres i de kørende versioner på netværket og at der foretages opdateringer herefter
- Begrænse adgangen til netværket til kun godkendte enheder og udstyr
- Implementer teknologier der giver mulighed for detektion af virus, botnet(netvært af inficerede computere), data-genkendelse og IPS(system til beskyttelse mod indtrængen) – som minimum på gateway niveau
- Etabler en løsning der sikrer sårbarheder detekteres i de kørende versioner på netværket og foretage opdateringer herefter

DELKONKLUSION KLIENTER

Væsentlige fund

Bærbare testes ikke af tredje part

Opsætning på bærbare testes typisk ikke af tredje part. Dermed har man ikke et fuldt indblik i den samlede sikkerhed på enhederne, hvilket betyder at det er umuligt at udtale sig om hvilken risiko man løber ved at benytte en given opsætning.

Ingen Kryptering af harddisk

Der benyttes typisk ikke fuld harddisk kryptering på bærbare. Det betyder, at malware har nemmere ved at eskalere sine rettigheder. Således vil evt. sensitive informationer relativt nemt kunne udtrækkes, hvilket gælder eksempelvis brugernavne, password til PCer, men også passwords til trådløs netværk osv.

DELKONKLUSION KLIENTER

Væsentlige fund

Medarbejder er administrator på deres computer

Det anses som fundamental dårlig sikkerhed at lade sine medarbejderes normale profil være administrator. Hvis computeren bliver inficeret, åbner det op for en lang række nye sårbarheder og som virksomhed bliver man ofte ramt hårdere af malware, hvis det rammer en profil som er administrator.

Ingen MDM-løsning

Når der ikke benyttes en Mobile Device Management (MDM) løsning kan man ikke sikre et ensrettet sikkerhedsniveau på sine mobil enheder. Dermed mister man mulighed for at risikovurdere på enhederne.

DELKONKLUSION KLIENTER

Væsentlige fund

- Sikkerheden/opsætning på enhederne testes ikke af tredje part
- Langt de fleste systemhuse benytter ikke kryptering af harddisk
- Langt de fleste systemhuse lader deres medarbejdere være administrator
- Har ingen MDM-løsning

Anbefalinger

- Foretag en årlig sikkerhedstest for at vurdere om klienten har det fornødne sikkerhedsniveau
- Overvej fuld kryptering
- Fjern administratorrettigheder
- Implementer en MDM-løsning
- Sikre bedre antivirus/malware

DELKONKLUSION WEB

Væsentlige fund

SSL trafik inspiceres ikke

Mangel på overvågningenssystemer der kigger ind i den krypterede trafik (SSL), der udgør over 60% af den samlede trafik, betyder at evnen til at kunne opdage og bremse et angreb er stærkt begrænset, da det meste malware (virus) og botnet i dag benytter sig af SSL

Der findes ingen DLP-løsning

Der er ingen systemhuse som har et automatisk (Data loss prevention) DLP system der kan genkende et mønster i filer der forlader virksomheden (som fx cpr, patientnummer o.s.v), hvilket betyder at der større risiko for at der kan opstå lækage af informationer.

DELKONKLUSION WEB

Væsentlige fund

Ingen sikkerhedstest af E-ydelser

Der bliver i langt de fleste tilfælde ikke udført sikkerhedstest på de E-ydelses adgang, som de fleste læger har på deres hjemmeside. Det betyder, at eventuelle sårbarheder ikke bliver lukket så hurtigt som de bør, og en ondsindet person vil kunne udnytte systemet igennem længere tid

Ingen two-factor på Exchange adgang

Ved ikke at benytte to-faktor identificering på outlook adgang, så giver det større mulighed for ondsindet personer at opnå adgang og udnytte denne adgang som springbræt videre ind i systemhuset

DELKONKLUSION WEB

Væsentlige fund

- SSL trafik inspiceres ikke
- Der findes ingen DLP-løsning
- Der gennemføres ikke sikkerhedstest på e-ydelser hjemmeside
- Outlook kan tilgås fra internettet uden to-faktor identificering

Anbefalinger

- Inspicer SSL trafik
- Monitorerer data der sendes ud fra netværk til internettet
- Gennemfør sikkerhedstest
- Begræns adgang til Outlook eller indfør to-faktor identificering

DELKONKLUSION MAIL

Væsentlige fund

- Outlook kan tilgås fra internettet
- Der fortages ikke regel gennemgang på for at se efter ondsindet regler
- En del benytter ingen to-faktor identificering på adgang til OWA

Anbefalinger

- Lave to-faktor identificering
- Regelgennemgang periodisk, minimum en gang årligt
- Vurdere behovet for at have en Outlook Web Access (OWA) adgang til rådighed

DELKONKLUSION MEDARBEJDERE

Væsentlige fund

Ingen awareness kampagner

Der bliver ikke afholdt formaliseret og løbende awareness kampagner af medarbejdere, men foretages ad hoc. Det betyder erfaringsvis, at der er større risiko for at medarbejdere bliver offer for et målrettet angreb

Procedure for rapportering af hændelser

I situationer hvor en medarbejder oplever en sikkerhedshændelse, er der i flere systemhuse ingen formel procedure omkring rapportering. Derudover er der de fleste steder ingen whistleblower ordning, som en medarbejder kan benytte sig af.

DELKONKLUSION MEDARBEJDERE

Væsentlige fund

- Der afholdes ingen awareness kampagner
- Medarbejdere har ingen formaliseret procedure for rapportering af hændelser

Anbefalinger

- Bør afholde regelmæssige awareness kampagner for at reducere sandsynligheden for at der opstår sikkerhedsmæssige hændelser, som er forårsaget af medarbejdernes uhensigtsmæssige adfærd
- Sikre at der findes en procedure for hændelser og at denne er kendt af medarbejdere

DELKONKLUSION PROCESSER

Væsentlige fund

Ingen faste sikkerhedstest

Der fortages i meget begrænset omfang sikkerhedstest, og ofte drejer det sig om meget simple scanninger. Men for at kunne opnå en tilstrækkelig sikkerhed, så er det nødvendigt at gennemføre dybtgående sikkerhedstest

Ingen SIEM løsning

De fleste systemhuse har ingen SIEM løsning. Det betyder, at en række hændelser som kan opdages ved hjælp af analyse af logfiler, kan bevæge sig ubemærket gennem netværket. Selv om der udføres en manuel gennemgang af logfiler, så har det vist sig ikke at være effektivt til at opdage angreb i tide. Dermed udsætter systemhuset sig for unødvendig risiko.

DELKONKLUSION PROCESSER

Væsentlige fund

Stor mangel på nedskrevne processer

Der er i en række systemhuse en stor mangel på nedskrevne processer, og en meget ad-hoc tilgang til IT-sikkerheden. Denne tilgang til sikkerhed er ikke forenelig med et godt og stabilt sikkerhedsniveau og vil ofte også have den betydning at det er personafhængigt.

Ingen to-faktor identificering

De steder hvor medarbejder skal tilgå informationer udefra, bør der altid være 2 faktor godkendelse, som fx sms, samt brugernavn og password. Sandsynligheden for at et lækket brugernavn og password kan benyttes, til at opnå adgang til det interne netværk, falder til meget tæt på nul, hvis der benyttes to faktor godkendelse. Det anses for best pratice i dag at benytte denne tilgang

DELKONKLUSION PROCESSER

Væsentlige fund

- Der findes ikke en proces, der sikrer systemer sikkerhedsvurderes inden de sættes i produktion
- Indsamlet logs fra systemer benyttes ikke til detektering af kritiske hændelser
- Der er ikke faste sikkerhedstest
- Der er generelt en stor mangel på nedskrevne processer
- Meget ad-hoc tilgang til sikkerhed
- Ingen multifaktor-validering af brugere udefra

Anbefalinger

- Bør gennemføre monitorering af indsamlede logs
- Overveje ISO27001 til at sikre, at alle processer bliver gennemgået og sikret
- Bør gennemføre sikkerhedstest med faste intervaller
- Benytte multifaktor-validering af brugere udefra

OPSAMLING

RISIKO I FORHOLD TIL PERSONFØLSOM INFORMATION

Overordnet vurdering

- Ud fra en gennemsnitlig og samlet vurdering, er sandsynligheden for at der skal indtræffe en hændelse ved et systemhus som medfører lækage af personfølsom information meget lille. Et målrettet angreb vil med stor sandsynlighed være målrettet den enkelte læge. Det skal dog indskydes, at skulle en hændelse indtræffe, er de enkelte systemhuse evne til at opdage et sådan angreb begrænset.

Forslag til forbedringstiltag

ezenta
Sikre rammer om IT

Risiko	Intern/ekstern sikkerhed	Sandsynlighed (Lav, middel, høj)	Forslag til forbedringstiltag	Effekt (Lille, middel, Stor)	Estimeret forbedringsbudget
Risiko for lavt sikkerhedsniveau med hyppige angreb eller andre uheldigheder.	Intern	Høj	**Løbende opdatering af IT sikkerhedspolitikken**	Stor	Som udgangspunkt ingen ekstern omkostning. 3 dages intern tid om året
Risiko for at angreb vil medføre langt større skade end hvis man havde et SIEM system, da man uden et sådan system ofte ikke er i stand til at opdage et angreb, og dermed får en ondsindet person langt længere tid til at påføre en virksomhed skade.	Intern og Ekstern sikkerhed	Høj	**Implementering af SIEM**	Stor	-fra 200 kr. pr. asset om året plus 2 dages konfiguration à 10.000 kr. Gennemsnits antal af asset 100 stk.
Risiko for, at man som virksomhed bliver ramt af et angreb, da nyeste generation firewalls beskytter mod en lang række af de angreb, man ser i dag	Ekstern	Høj	**Implementering af next generation firewall**	Stor	-fra. 50.000 i indkøb plus standardkonfiguration og løbende årlige omkostninger på 10.000 kr. i hardwaresupport
Risiko for at der findes en sårbarhed på en klient som gør at den ikke er modstandsdygtig overfor malware eller andet ondsindet angreb	Ekstern	Middel	**Optimering af klient sikkerheden**	Middel	-300,- pr. arbejdsstation pr. år + 2 dages installationstid ved antal op til 50 brugere
Risiko for ondsindet person kan gætte eller på anden måde bryde et password som en medarbejder benytter	Intern	Lille	**Skift til password med minimum 12 tegn**	Stor	-0,- kr. i eksterne omkostninger. 1 times internt arbejde
Risiko for, at der findes en sårbarhed i et internet-vendt system, som kan give en ondsindet person adgang til det interne netværk	Ekstern	Middel	**Foretag løbende scanninger af perimeteren**	Middel	-15.000 kr. årligt
Risiko for at der findes en sårbarhed i et internet-vendt website, som kan give en ondsindet person adgang til det interne netværk	Ekstern	Middel	**Foretag løbende sikkerhedstest af website**	Middel	-40.000 kr. årligt
Risiko for at en ondsindet person kan lokke en medarbejder til at klikke på et ondsindet link, eller på anden måde få en medarbejder til at give fortrolige informationer til en ondsindet person	Intern	Høj	**Afhold regelmæssige awareness kampagner**	Stor	-fra 30.000 kr. årligt
Risiko for at nogen enten bevidst eller ubevidst kommer til at sætte ondsindet eller sårbart udstyr på netværket og dermed giver en ondsindet person adgang til netværket	Ekstern	Middel	**Begræns adgangen til netværket til godkendte enheder og udstyr**	Lille	-fra 30.000 kr. I engangsinvestering plus løbende årlige supportomkostninger