Øving - 23

Eric Younger
Thomas Bakken Moe
Jonas Brunvoll Larsson

Oppgave 1

Les artiklene om Multiconsult og Barclays. Svar så på følgende:
a) Hva kunne de gjort for å forhindre at dette skjedde?
b) Hvilke skademinimerende tiltak kan du se for deg hadde vært nyttige?

Svar:

Multiconsult

I Multiconsult saken så blir spørsmålet blir hvorvidt den tyngste sikkerheten skal ligge, er det økonomiske tap over tapte pcer, eller beskyttelse av sensitiv informasjon. Uansett så virker det ut som Multiconsult ikke sikret for hverken av delene.

Multiconsult kunne gjort flere fysiske sikringer for å forhindre innbruddet, de kunne hatt forsterkede dører med bedre låser, med digital lås som kun kan låses opp med nøkkelkort f.eks. Det at innbruddstyven kunne bryte opp døren raskere enn å låse opp med nøkkel på samme tid viser at døren ga lite sikkerhet.

Hvis Multiconsult hadde sensitiv informasjon på laptopene, så kunne de også ha vurdert å låse inn laptopene i et hvelv etter stengetid, eller ihvertfall sikret de noe mer. De kunne også benyttet seg av laptop låser, som kun kan åpnes med en nøkkel. Spesielt med slike låser hvor dersom man prøver å rive ut låsen så river den med en bit av hovedkortet i tillegg. Videre så bør harddisker også krypteres slik at tyvene ikke bare kan ta ut harddisken og sette den inn som en ekstern harddisk til en annen pc.

Barclays

Den store feilen som ble begått var at Barclays ga de kriminelle fysisk tilgang til systemene sine. Dette vitner om at Barclays trenger rutiner om hvem som for lov til å håndtere hvilket utstyr.

I Barclays saken kunne innbruddet vært forhindret om Barclays hadde hatt er mer bevisst forhold til sikkerhetsrutiner. Det hjelper lite å ha gode fysiske sikringer (dører, låser) og sikker programvare, når det finnes lette måter man kan komme seg rundt hindringene.

Før en teknikker i det hele tatt får tilgang til maskiner med sensitiv data, burde Barclays forsikre seg om at det faktisk er et behov for en teknikker i det hele tatt. Hvilken tekniske problemer ere meldt inn? Om problemet som teknikeren oppgir ikke er rapportert inn, burde heller de ikke bli satt i arbeid uten videre. Et naturlig steg er å forhøre seg med Barclays sikkerhetsansvarlige.

Det er ikke sikkert å gi alle ansatte og eksterne entreprenører tilgang til sensitive data og systemer. Her burde det vært stilt større krav til autentisering av hvem som har lov til å jobbe på maskiner med sensitiv informasjon og om det er meldt inn noen feil. Man kan for eksempel kreve at noen fra firmaets interne IT-mannskap skal være med eksterne entreprenører når de jobber.

Oppgave 2

Fortell om en eller annen sikkerhetshendelse eller et sikkerhetsproblem du/dere har opplevd eller hørt om. Her er mange muligheter:

• Noe som har skjedd, alt fra målrettet angrep til datatap/nedetid.
• Et usikkert opplegg eller dårlige rutiner. Det behøver ikke ha skjedd noe, men risikoen har vært «for stor» etter ditt syn.

Gjør deretter rede for hvordan dette kunne vært håndtert bedre. Hva ville du gjort for å unngå problemet, om det var du som bestemte?

Svar:

Dagen da serveren frøys

Selsbakk ungdomsskole var en testskole hvor man prøvde å bruke datamaskiner i undervisningen i større grad enn på andre skoler (perioden 2008-2011*). Det var 100-200 stasjonære maskiner som var plassert i datasaler på skolen. Maskinene var egentlige bare skall. Selve operativsystemet kjørte på en stor felles server. Serveren var også ansvarlig for alt av lagring. Operativsystemet var unix-baserte Skolelinux**. Dette tekniske systemet var naturligvis noe som skolen var ganske stolte over. For å vise seg fram (og kanskje vekke litt interesse blant elevene), var den sentrale serveren plassert i et rom med glassvegger i øverste etg. I tillegg til å være på utstilling for hele skolen, hadde serveren også et eget ventilasjonsanlegg, separat fra resten av skolens VVS, for å holde seg kjølig. Alt dette gjorde det ekstra pinlig, når elevene en vinterdag i 2009 kom inn til synet av serveren druknet i over 1 meter snø, og en stakkars IT-ansatt som sto der med spade og bøtte. Det ble ikke noen bruk av Skolelinux den dagen.

Selsbakk skole ble grunnlagt i 1977 og var derfor ikke designet til å kunne huse servere og mange datamaskiner. Da det sikkert høres flott ut å ha et helt eget ventilasjonssystem for serverrommet, så var dette noe som ble lagt til i etterkant. Dette nye ventilasjonssystemet var nokk ikke bygget til de samme standardene som hele byggets VVS. Blant annet besto systemet av et rør som gikk direkte i fra det flate taket, og ned til serverrommet. Røret var dekket over av inntaket på taket, men etter stort snøfall, hadde dette gitt etter og rast nedover det rette røret, rett inn i serverrommet.

Det Selsbakk skole kunne ha gjort bedre i denne situasjonen er flere ting. De kunne ha installert et mer robust ventilasjonssystem. Taket var flatt, og området hvor

skolen er, er ikke ukjent med store mengder våt snø om vinteren. Da ventilasjonssystemet ble laget, kunne de ha satt inntaket på siden av bygningen, i stedet for på taket. Om de måtte ha inntaket på taket, kunne man ha hatt et mer solid bygd inntak og/eller ikke hatt et rett rør som går fra inntaket til serverrommet (slik at det ikke blir en direkte vei fra snøen på taket inn til serverrommet).

Skolen kunne også hatt en backup-server på en annen plass i bygget eller off-site, slik at om hovedserveren går ned, så har man et alternativ. Dette er riktignok en ganske kostbar løsning.

Notater:
** Dette er perioden når Thomas Bakken Moe gikk på skolen, det er usikkert hvor lenge før/etter denne perioden prøveprosjektet varte.*
*** https://en.wikipedia.org/wiki/Skolelinux*

Oppgave 3

Du som har hatt dette faget, har sikkert noen idéer om hvordan sikkerheten kan gjøres bedre!

• Gjør rede for alle problemer du ser. Ledelsen er med på sikkerhetstiltak, men de er såpass oppegående at de vil vite «hvorfor».

• Gjør rede for sikkerhetstiltak, forandringer og nytt utstyr/programvare. Tegn opp hvordan du mener det nye nettet bør være. Det er fint om eksisterende måter å bruke nettet kan føres videre, men selvfølgelig på en sikrere måte enn i dag.

• Lag et kort utkast til en sikkerhetspolicy, og fortell om hva du vil kurse de ansatte i, angå-ende nettsikkerhet.

• Gjør rede for hvilke regler du vil ha i brannmuren. Hver brannmur-regel skal begrunnes, med en kort forklaring på hvorfor den hjelper.

Svar:

Problemer med systemet i dag og våre løsninger:

- **Problem 1**:
  Bedriften skiller ikke mellom ansatt-nett og kunde-nett.

  Løsning 1:
  En mulig løsning er å sette opp to ulike wifi-nett. Et nett for ansatte og et nett for kunder. Det er ingen grunn til at kunder skal ha tilgang til alle ressursene som ansatte i bedriften har. Jo mindre kunden har tilgang til, desto tryggere er det for bedriften.

- **Problem 2:**
  Bedriften har alt av tjenester og maskiner på samme nettverk uten å skille av.

  Løsning 2:
  Det bør settes opp en demilitarisert sone slik webtjener, mailtjener o.l er sikret på nettverket i en egen sone, bak en brannmur. Så bør filtjenere og de ansattes datamaskiner kobles på nett som ligger bak enda en brannmur til. Man unngår da at en kan hacke seg inn i en pc på nettet og ha tilgang til all data og tjenester som bedriften har.

De bør også omstrukturere nettet slik at man benytter seg av en VPN for å få tilgang til filtjener og slikt på ansatt nettet gjennom Wifi og fra hjemmekontor/reise.

Så bør det kablede nettverket ha 802.X autentisering, og for ekstra sikkerhet benytte seg av MAC filtrering for å unngå at noen skal finne en ledig ethernet plugg og dermed ha tilgang til alt.

- **Problem 3:**
  Brannmuren er gammel og ingen vet hvordan den fungerer.

  Løsning 3:
  Kjøp ny, lag god dokumentasjon på hvordan den fungerer og lær opp flere ansatte i hvordan systemet henger sammen.

- **Problem 4:**
  Bedriften hadde problem med ødelagte websider.

  Løsning 4:
  Bedriften bør begynne å ta i bruk et distribuert versjonskontrollsystem. For eksempel, Git. Med et versjonskontrollsystem kan man lett rulle tilbake til en fungerende versjon om noe i systemet ikke fungere som det skal.

- **Problem 5:**
  Tidligere server ble ødelagt på grunn av vannskader fra varmtvannstank og mye data/tid gikk tapt.

  Løsning 5:
  Dette kan forhindres flytte serverrommet og/eller sikre taket i serverrommet mot lekkasje. Bedriften bør også vurdere å å installere sensorer for å overvåke temperatur, fukt, og støvmengde på serverrommet. På den måten kan man varsles tidlig hvis forholdene på serverrommet er utenom det normale. Et annet godt tiltak er å løse serveren inne i serverskap. På den måten sikrer man blir det vanskeligere for noen uten adgang å tukle med serverene.

  Bedriften bør også inngå avtale med et firma som driver med offsite backup. Da vil all data på serveren periodisk blir sikkerhetskopiert til en annen

lokasjon. Om bedriften får et katastrofalt tap av data igjen, vil det være relativt lett å få dataen tilbake.

- **Problem 6:**
  Det er mangel på gode rutiner for sikkerhet og regler for deling av informasjon. Dette kan føre til at hemmelig informasjon lekker og/eller rot da man har delte filer spredt utover flere skylagringstjenester.

  Løsning 6:
  Bedriften må først og fremst bestemme seg for hvilke skytjenester som er godkjente for ansatte å benytte seg av. De ansatte skal ikke benytte seg av egen valgte eksterne løsninger, hvor bedriften ikke har kontrakt med selskapet som tilbyr løsningene. Data kan bli brukt og solgt videre av sky selskapet om det er ikke foretatt en sikkerhetsvurdering av tjenesten. Videre må bedriften komme med tydelige retningslinjer på hvordan skytjenestene skal brukes. Disse retningslinjene skal være tydelig beskrevet i bedriftens sikkerhetspolicy.

- **Problem 7:**
  Treg nettlinje opp mot filtjener og andre tjenester. Her ligger nok problemet enten i at selve filtjeneren er treg (mulig utdatert hardware) og/eller nettlinjene til/fra filtjeneren.

  Løsning 7:
  Fikse hastighet opp mot filtjener og andre tjenester, så det blir brukbart for de ansatte, og de ansatte slipper å ta snarveier for å kunne jobbe effektivt og sikkert.

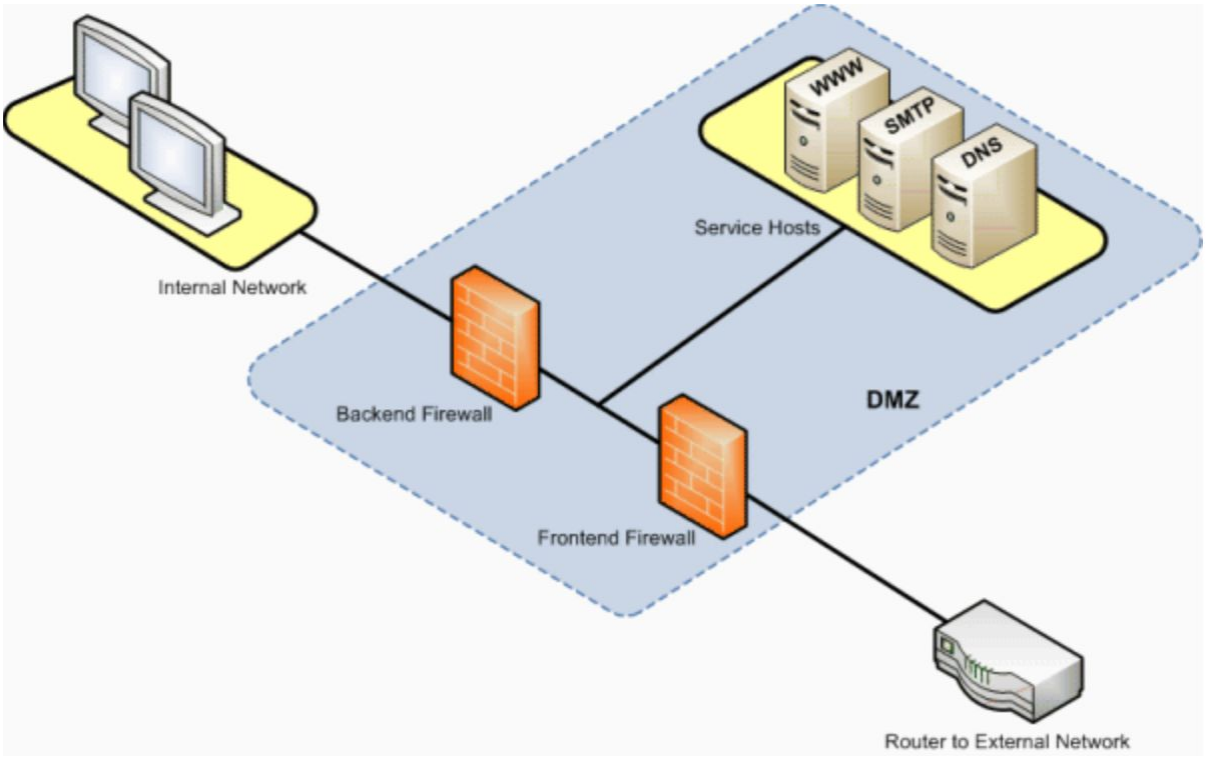
  Om det er selve filtjeneren som er treg, kan man fikse dette med innkjøp av ny hardware. Om man går til innkjøp av ny filtjener, bør funksjonaliteten til denne dokumenteres godt og de ansatte må læres opp i bruken av den.

  Om det er nettlinjene som er problemet, kan man gå til innkjøp av 10Gb nettverksutstyr eller dedikerte fiberlinjer.

- **Problem 8:**
  Konkurrenter stjeler kunder med billigere priser. Dette er ganske selvsagt et problem bedriftsmessig.

Løsning 8:
I og med at en konkurrent har lignende priser, bare litt billigere, og i tillegg til at nettsider blir ødelagt, så skal man ikke se vekk ifra bedrifts spionasje/sabotasje. Rutinekontroll med antivirus for å sjekke etter trojanere, keyloggers, og uvedkommende på nettverket må til. Videre så kan det være aktuelt å sette opp NIDS, og evnt IPS for å beskytte mot uvedkommende.

Tegning av det nye nettverket



Det trengs ikke mye nytt utstyr, man trenger bare to brannmurer for å dele opp nettverket inn i forskjellige soner.

Utkast til en Sikkerhetspolicy
Formål med sikkerhetspolicyen er å utarbeide gode rutiner som ivaretar bedriftens sikkerhet og sikkerheten til de ansatte.

1. Generelle sikkerhets prinsipper
    - Passord og brukernavn skal aldri deles med noen.
    - Ved mistanke om et sikkerhetshull/feil skal IKT-avdelingen varsles umiddelbart.
    - Programmer skal sikkerhetsklareres før de installeres på jobbmaskin.

2. Regler for bruk av VPN
    - VPN skal benyttes om man jobber hjemmefra, på wifi, eller off-site.
    - Man logger på VPNen for å jobbe. Når man er ferdig med å jobbe, logger man seg av.

3. Regler for utvikling av programvare
    - Kode skal aldri deles med noen utenfor bedriften.
    - Kode skal aldri lagres i et tredjepartsverktøy utenom verktøy som er godkjent av bedriften.
    - Synkroniser jevnlig med master branch. På den måten unngår man store konflikter i koden.
    - Utviklingsarbeid skal alltid foregå på egne brancher. Ikke på master - branchen.
    - En oppdatering skal testes og godkjennes av minst en annen utvikler får den pushes ut på master branchen.

4. Regler for kommunikasjon med kunder
    - Det er kun dokumenter som er godkjent for kundedeling, som skal deles med kunder.
    - Del aldri flere dokumenter med kunden en det som er nødvendig.

5. Rollefordeling
    - Det er kun ansatte fra IKT-avdelingen som har tilgang til serverrommet.
    - Det er kun ansatte fra IKT som har administratortilgang på filtjeneren, mail-tjeneren, VPN-tjeneren, og alt av nettverksutstyr.

Nyttige kurs for de ansatte
Det finnes en rekke kurs de ansatte kan delta på som kan være nyttige for bedriften. I første omgang er nok det viktigste å arrangere kurs som sikrer at de ansatte skjønner viktigheten av de nye sikkerhetsrutinene og hvorfor bedriften har kommet med en ny sikkerhetspolicy. Når de ansatte skjønner viktigheten bak sikkerhetstiltakene, vil det være enklere for dem å akseptere omstillingen.

Videre bør det arrangeres kurs som viser hvordan de nye verktøyene fungerer. To gode eksempler her er bruk av VPN og bruk av bedriftens versjonskontrollsystem. Med skikkelig innføring i hvordan verktøyene fungerer vil sannsynligheten for feil minske. Trolig vil flere av de ansatte benytte seg av de nye verktøyene og ikke komme opp med egendefinerte løsninger, hvis de får en skikkelig innføring fra starten av.

Verktøyene bedriften benytter seg av kommer trolig med oppdateringer jevnlig. Bedriften bør stille krav til de ansatte om at de prøver å holde seg oppdatert. Det bør også arrangeres oppdateringskurs med jevne mellomrom. På den måten kan bedriften forsikre seg om at de ansatte i bedriften er oppdatert.

Bedriften bør også oppfordre til, og legge til rette for kunnskapsdeling mellom de ansatte. Slik slipper bedriften å miste mye kritisk kompetanse hvis ansatte slutter.

Brannmur for det interne nettet:
Vi vil blokkere all inngående trafikk inn til beskyttede tjenester som filtjener, server-rack osv som standard, men heller åpne opp for at trafikk gjennom ip-adressen til VPN og trafikk gjennom ethernet porter som er autentisert skal få slippe gjennom.

Regler	**Kommentar**
"iptables -P FORWARD DROP"	**Dropper alle pakker som skal videresendes. Skal ikke fungere som en ruter.**
"iptables -P INPUT DROP"	**Denne linjer dropper all innkommende trafikk som vi ikke eksplisitt godtar.**
"iptables -P OUTPUT ACCEPT"	**Tillate utgående trafikk. Kan ha tjenester som trenger å hente informasjon på vegne for oss.**
"iptables -A INPUT -i lo -j ACCEPT"	**Tillate localhost å sende og motta pakker, f.eks ha en server kjørende.**

"iptables -A INPUT -s XXX.XXX.X.XX -j ACCEPT"	**Godtar bare innkommende trafikk fra VPN ip addressen.**
"iptables -A INPUT -i eth1 -s 10.50.0.0/16 -j ACCEPT"	**Godtar bare innkommende trafikk fra ethernet.**
"sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT"	**Godta relaterte og allerede opprettede forbindelser til å sende svar pakker tilbake igjen.**

Regler for brannmur for demilitarisert sone:

Regler	Kommentar
"iptables -A FORWARD -i eth0 -o eth2 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT"	**Videresende trafikk mellom DMZ og LAN**
"iptables -A FORWARD -i eth2 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT"	**Videresende trafikk mellom DMZ og LAN**
"iptables -A FORWARD -i eth2 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT"	**Videresende trafikk mellom DMZ og WAN servere som SMTP, Mail osv.**
"iptables -A FORWARD -i eth1 -o eth2 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT"	**Videresende trafikk mellom DMZ og WAN servere som SMTP, Mail osv.**
"iptables -t nat -A PREROUTING -p tcp -i eth1 -d 202.54.1.1 --dport 25 -j DNAT --to-destination 192.168.2.2"	**Rute innkommende trafikk på port 25 til DMZ server 192.168.2.2**
"iptables -t nat -A PREROUTING -p tcp -i eth1 -d 202.54.1.1 --dport 80 -j DNAT --to-destination 192.168.2.3"	**Rute innkommende trafikk på port 25 til DMZ server 192.168.2.2**
"iptables -t nat -A PREROUTING -p tcp -i eth1 -d 202.54.1.1 --dport 443 -j DNAT --to-destination 192.168.2.4"	**Rute innkommende trafikk for HTTPS på port 443 til DMZ server med reverse load balancer på IP 192.168.2.4**