Säkerhetsnätverket

Minnesanteckning / sammanfattning

Säkerhetsnätverkets nätverksträff 8/10 2019
Central Hotel, Vasagatan 38, Stockholm
Tema: Organisationens digitala perimeter
Närvarande: Annika Salomonsson, Thomas Drugge, David Åström, Patrik Olsson, Roger Stolt, Oscar Wide (medföljande), EvaLotta Wahlström (Nätverksledare)

08:30 Välkommen! Introduktion och presentationsrunda.

Vi fick lite mer tid att presentera oss den här gången med syfte att bygga förtroendet i gruppen. Det var många som tyvärr inte kunde närvara denna träff vilket ledde till en fundering. Fördelen med Säkerhetsnätverket i jämförelse med många andra nätverk är att medlemskapet tillhör verksamheten – dvs en kollega till dig får delta i ditt ställe. Vi konstaterade att det är viktigt att du som medlem försöker hitta en ersättare till träffarna om du inte själv kan närvara - detta för att det ska bli så givande som möjligt för de som deltar.

Dagens föreläsare var Oliver Rickfors:

Oliver Rickfors är säkerhetsteknisk analytiker och arbetar som penetrationstestare på Knowit Secure med inriktning på IoT som attackvektor och perimetertester. Han utbildar och föreläser för bolag och högskolor för att öka medvetenheten till potentiella hot och digitala attackvektorer inom organisationen. Oliver har en bakgrund inom finansbranschen med systemutveckling/security operations och penetrationstestar idag på heltid.

Program

Oliver föreläste på ämnet Organisationens digitala perimeter - hur hotet ser ut från Internet och berörde följande punkter:

- Attackvektorer och infiltreringsmetoder
- Exempel på attacker / incidenter
- Aktörernas profiler
- Åtgärdsförslag

Min personliga reflektion från det Oliver och gruppen pratade om:

Även välinformerade och kunniga tekniker kan råka ut för en attack och nappa på phishing om den är vältajmad och sofistikerad. Oliver berättade hur nära han var att klicka på en länk från ”Post Nord” som aviserade att han mottagit ett paket som han faktiskt väntade på.

Noterade att IoT (Internet of Things) – innebär att en ljusknapp idag faktiskt är en liten dator och inte bara en av-och-på knapp, precis som ventilationen och en kaffemaskin. Och dessa utgör en risk och erbjuder en möjlighet till intrång. Fler exempel var kopiatormaskin.

Spännande att få veta lite om de som gör intrång och anledningarna. Att de arbetar snabbt och hur man än försöker patcha och täppa till hålen i operativsystem så är de snabba att plocka isär de patcharna. Men viktigt att uppdatera och gör det fort när det erbjuds!

Det vanligaste tillvägagångssättet för intrång som rapporteras vid incidenter är Social engineering / Phishing.

En fråga från gruppen var: Var i ligger den största sårbarheten för intrång?
”IT-säkerhet är enkelt om man tar bort människan.” blev svaret.

Hur gör man för att förebygga intrång?

Man kan t.ex. införa en ”Sanity check” (Hur vet man att mailet kommer från rätt person? Hur vet man att filen som laddas upp i ett system inte har virus?) Jag bad Oliver om en länk - https://en.wikipedia.org/wiki/Sanity_check/ uppnås genom utbildning kräver att tid/pengar budgeteras i utvecklingsprocessen.

Utbilda – skapa awareness. En medlem berättade om hur de i organisationen har t.ex. gett medarbetarna små stickers (ögonlock) för datorernas kameralins, när man loggar på sin datorn kommer en iögonfallande notis där det står en uppmaning till försiktighet.
Händer något nyhetsmässigt så använd det för att få medarbetarna uppmärksamma på riskerna.

Organisationen bör exempelvis ha en incidentrapporteringsportal eller veta hur saker ska rapporteras.

Det konstaterades att det är kostsamt med it-säkerhet och att kostnaderna för incidenter är svåra att beräkna. En av deltagarna uttryckte att det vore önskvärt att göra en revision på informationssäkerheten i organisationen – en ordentlig analys som lyfter allt till ytan och belyser var åtgärder behövs.

Sammanfattningsvis: bästa sättet att förebygga incidenter / intrång är att se till att man har nyckelpersoner, utbildning / awareness och att se till att man har flera skyddslager.

Olivers kontaktuppgifter: Oliver.Rickfors@knowit.se Mobil 0722-432 642

Datum för kommande nätverksträffar: 12/11 (kl 13-17) därefter mingel och avslut för nätverkets första år!

OBS! Dokumentationen från nätverksträffarna är ämnat för att ni ska kunna förmedla informationen internt. Namn på deltagare och information om vad som sagts i förtroende på mötet får inte spridas.

Bilagor
Organisationens digitala perimeter
Bilder från träffen