Säkerhetsgranskning krav pum grupp fem

Jon Dybeck

2014-03-14

1 Förord

Vi utvecklar ett träningssystem för personal inom räddnings och sjukvårdspersonal. Vår kund, Katastrofmedicinskt centrum (KMC) bedriver övningar för denna yrkesgrupp för att förbereda personalen inför eventuella riktiga katastrofer.

Men vårt system kommer inte att användas under verkliga katastrofer utan endast för utbildning. Systemet är tänkt att användas på ett skyddat intranät som ej är exponerat mot internet.

Men även i denna skyddade miljö finns det en mycket viktig tillgång som måste skyddas, allt träningsmaterial som används i övningarna. Detta material lagras på servern och ska normalt inte lämna denna.

Det är även viktigt att skydda KMCs datornätverk från attacker som börjar i vårt system eftersom nätverket kommer att användas under skarpa händelser, även om inte just vårt system används då.

2 Riskanalys

2.1 S.R.1.3

2.1.1 Asset

Datorn som användaren sitter vid, datornätverket den är ansluten till.

2.1.2 Actor

Användaren som använder programmet.

2.1.3 Misuse scenario

Ett hot skickar en korrupt fil som använder en exploit i editorns fil-inladdningskod. Vilket kan tex leda till att hotet får tillgång till användarens dator.

2.1.4 Probability

Possible

2.1.5 Impact

Serious

2.1.6 Risk

Medium

2.1.7 Mitigation

Använd ett standardiserat format (xml) för scenariofiler och använd Microsofts standardiserade bibliotek för att ladda data från filer. Biblioteken används av många och är vältestade, xml inehåller få features som kan användas i en exploit.

2.2 S.R.22.1

2.2.1 Asset

Serverdata

2.2.2 Actor

Handledaren som laddar ett scenario via managern.

2.2.3 Misuse scenario

Ett hot skapar en korrupt scenariofil och skickar denna till en handledare. Handledaren laddar sedan in scenariot via managern till servern. Den korrupta filen inehåller sedan en exploit som till exempel kopierar den data som lagras på servern och skickar denna till tredje part.

2.2.4 Probability

Possible

2.2.5 Impact

Catastrophic

2.2.6 Risk

Medium

2.2.7 Mitigation

Åter igen, använd ett standardiserat format och standardbibliotek för all laddning av filer.

2.3 S.R.37

2.3.1 Asset

Datorn editorn körs på, datornätverket.

2.3.2 Actor

Handledare

2.3.3 Misuse scenario

Ett hot utför en man-in-the-middle attack mot editorns google-maps anslutning och utnytjar en exploit i editorns karthantering.

2.3.4 Probability

Almost impossible

2.3.5 Impact

Negligible

2.3.6 Risk

Informational

2.3.7 Mitigation

Informera beställaren om den teoretiska risken. Eftersom anslutningen är krypterad är det osannolikt men inte omöjligt att detta kommer ske.

2.4 A.R.37

2.4.1 Asset

Servern under en övning.

2.4.2 Actor

Handledare.

2.4.3 Misuse scenario

Ett hot skapar ett stort antal manager anslutningar till servern under en stor pågående övning. Detta leder till denial of service vilket leder till stora förseningar under övningen.

2.4.4 Probability

Possible

2.4.5 Impact

Bearable

2.4.6 Risk

Low

2.4.7 Mitigation

Specificera i kravspecifikationen att servern alltid skall vara installerad på ett skyddat nätverk bakom en brandvägg så att externt hot ej kan nå servern.

2.5 S.R.21

2.5.1 Asset

Server

2.5.2 Actor

Handledare

2.5.3 Misuse scenario

En ondskefull handledare konfigurerar servern att öppna sig för anslutningar från ett externt nätverk och låter utomstående ansluta till servern. Dessa laddar sedan ned emergo train system data från servern.

2.5.4 Probability

Possible

2.5.5 Impact

Catastrophic

2.5.6 Risk

Medium

2.5.7 Mitigation

Skriv tydligt i systemdokumentationen att systemet skall installeras bakom en brandvägg som ej tillåter kommunikation mellan servern och externa nätverk. Varken med servern som källa eller destination.

2.6 A.R.45

2.6.1 Asset

Serverdata

2.6.2 Actor

Användare och handledare

2.6.3 Misuse scenario

Ett hot kommer över gamla inloggningsuppgifter till digimergo server systemet och loggar in. Denne laddar sedan ned emergo train system data från servern.

2.6.4 Probability

Possible

2.6.5 Impact

Catastrophic

2.6.6 Risk

Medium

2.6.7 Mitigation

Använd Microsofts domänsystem för att hantera alla inloggningsuppgifter istället för att implementera detta i digimergo. På detta sätt hålls användarkontona uppdaterade enligt kundens egen säkerhetspolicy.

3 Feedback

3.1 Fördelaktigt?

Ja, eftersom vårt system kan komma att placeras i en miljö där det finns andra kritiska system tycker jag att det var bra att utföra denna undersökning.

3.2 Tidsåtgång

Ungefär fyra timmar på en person.

3.3 Kunskap

Jag är relativt uppdaterad på olika säkerhetsområden, särskillt inom nätverksprotokoll.

3.4 Identifierade risker

Jag hittade fem fårvånansvärt allvarliga risker som jag kommer att ta upp med vår kund. Främst för att skydda deras nätverk eftersom detta är en viktig sammhällsfunktion.

3.5 Generell feedback

Jag tycker att denna föreläsning och uppgift är välldigt viktig, av två anledningar. Vi har inte haft någon riktig kurs om säkerhet, det har nämnts men det är bra att få en repetition. Särskillt eftersom vissa av de system som skapas under kursens gång kommer att användas av en kund. Då är det viktigt att systemet faktiskt har utvärderats ur en säkerhetssynpunkt.