Högskolan i Halmstad, VT16
Webbsystem och IT-säkerhet, 7,5hp
Christopher Wohlfarth, 931004
chrwoh14@student.hh.se

Hemtentamen

Datum: 21-03-2016
Lärare: Margaretha Eriksson, Jesper Lund

Uppgift 1 (30 p)

Sammanhang
För att kunna göra en riskanalys av Abelix ABs webbapplikation så krävs det att en del information kring företagets och webbapplikationens omgivning och miljö samlas in. Denna informationen kommer ge oss ett sammanhang av generella observationer kring säkerhet som hjälper oss när vi skapar riskanalysen.

Vad vi vet
- Abelix vill gå över från postorderförsäljning till renodlad e-handel.
- De vill att 80% av försäljningen ska ske via den nya webbshopen.
- Kunder hittar produktutbud via papperskatalog eller digital katalog via e-post.
- Abelix har ett datornätverk som består av ett par servrar.
- Det finns en server där affärssystemet körs med fakturering, lagerhantering, budgetering, kundregister och redovisning.
- Det finns en webbserver och en e-postserver.
- All datorutrustning finns i Abelix lokaler som är en del av en företagspark(andra företag har kontor i samma lokaler).
- Hemsidan med webbshopen presenterar produkter och innehåller ett kontaktformulär som nya kunder ska fylla i.
- En inloggningsfunktion ska införas så att registrerade kunder ska kunna få specialerbjudanden, rabatter och möjlighet till direktbetalning via kreditkort. Inloggningsfunktionen ska byggas av en släktings dotter till VDn.
- Servrarna är två år gamla och underhålls av en lokal leverantör som inte har någon personal med kompetens för IT-drift eller informationssäkerhet.
- Webben sköts just nu av Nicolas som nyligen har ansökt om tjänstledigt i två år. Han har byggt webbshopen och är den som vet hur allt fungerar, han är den som fixar till det när webbshopen inte fungerar.
- Det finns en kort instruktion om hur man lägger till och uppdaterar produkter på webbshopen.

Observationer
- I webbshopen förekommer samma produkt flera gånger, fast med olika pris. Anledningen till detta är för att det är komplicerat för Nicolas att ta bort gamla produkter.
- Det finns ett administrationsprogram för att redigera databasen men Nicolas har glömt lösenordet till det.
- På sistone har det varit flera oförklarliga stopp på webbshopen, ”sidan har låst sig”. En provisorisk lösningen till detta har varit att Nicolas startat om webbservern.
- Kunddatabasen har visat sig numera innehålla en omfattande mängt användare, både riktiga användare, men också sådana som ”kalle.anka@abelix.se” som ingen på företaget känner igen.
- Produktdatabasen har vuxit kraftigt och innehåller nu flera varianter av samma produkt, fast med olika priser och leverantörer. Anledningen till detta är för att det beror på när produkterna har köpts in.
- Grunddatan för produkter finns i affärssytemet som ligger på en separat server av säkerhetsskäl. Det innebär att Nicolas måste manuellt uppdatera webbshopens produktdatabas om något ändras i affärssytemet.
- Eftersom anställda på företaget visas på hemsidan så händer det nu att de får spampost till sina brevlådor i e-post.
- Nyligen har externa skadliga mejl spridit sig inom företaget vilket har lett till att nätverket har havererat. Kunder har sedan detta haveriet rapporterat att webbshopen är obrukbar.

Riskanalys

Nedan visas en tabell innehållande incidentscenarion(d.v.s. risker, potentiella sårbarheter och hot) som är baserade på den information vi har fått tillgång till från Abelix. För varje scenario uppskattas riskens sannolikhet(1-10) och påverkan(1-10), där 1 är väldigt osannolikt/låg påverkan och 10 är extremt sannolikt/ hög påverkan (Tonnquist, 2012; Shems, 2011). Baserat på dessa två bedöms till sist den uppskattade risken(sannolikhet x påverkan, 1-100), ju högre värde desto allvarligare är risken (Tonnquist, 2012; Shems, 2011). Baserat på denna informationen kan sedan riskerna rangordnas för att bl.a. ge en grund till en åtgärdsplan (Shems, 2011).

Incident	Sannolikhet	Påverkan	Uppskattad risk
Webbshopen visar fel produkter med fel pris vilket leder till att kunder blir missnöjda.	10	8	80
En obehörig person får tillgång till administrationsprogrammet för att redigera databasen eftersom Nicolas har slarvat bort lösenordet.	3	10	30
Webbshopen låser sig så att kunder inte kan använda sajten.	8	10	80
Kunddatabasen blir attackerad och känsliga uppgifter sprids till allmänheten.	5	10	50
Nicolas för in fel produktinformation i produktdatabasen från affärssytemet.	8	8	64
Anställda utsätts för phising-epost som kan leda till intrång i både affärssystem och webbshopens databas.	5	10	50
Abelix två år gamla servrar havererar, det finns inga reserv-servrar som ersättning. Ingen med IT-kompetens kan hjälpa till.	6	10	60
En utomstående person i företagsparken smyger sig in i Abelix serverrum och attackerar affärssystemets servrar och får tillgång till fakturering, lagerhantering, budgetering, kundregister och redovisning.	4	10	40
Inloggningsfunktionen som byggs av en släktnings dotter till VD har säkerhetshål i sig. Funktionen blir attackerad och kunder blir hackade, de får felaktiga specialerbjudanden, rabatter, och kan förlora sina bankuppgifter.	7	10	70
Kontaktformuläret på webbshopen utsätts för SQL-injections vilket raderar data ur databasen. Alternativt cross-site-scripting som även skadar webbshopen.	6	9	54
När Nicolas tar tjänstledigt så finns det ingen på företaget som kan underhålla webbshopen, detta skapar problem.	9	7	63
Det blir översvämmning i serverrummet på företagsparken, det finns inga reserv-servrar på extern plats.	3	9	27
Eftersom produktdatabasen innehåller felaktig data så blir det väldigt många felbeställningar från kunder. Detta skapar koas i både webbshopens databas och Abelix affärssystem.	7	10	70
En anställd på Abelix glömmer sin smarta telefon på en restaurang en lördagkväll. Telefonen hittas av en utomstående person som får tillgång till inloggningsuppgifter och annan känsligt information om Abelix verksamhet.	3	7	21
Webbshoppens betalfunktion blir attackerad, kunders bankinformation sprids till utomstående personer.	4	10	40

RSA-rapport

Nedan är en kort risk- och sårbarhetsrapport som beskriver och sammanfattar riskanalysen som har utförts. Denna rapporten kommer läsas av Abelix VD, chefer, ansvariga tekniker o.s.v. Rapporten ger Abelix ledning en bra översikt och förståelse för vilka IT-hot och sårbarheter som de är känsliga för. Efter att de läst denna rapporten samt tagit del av en åtgärdsplan kan de agera och bestämma hur de vill gå vidare i arbetet kring deras IT-säkerhet.

Kort beskrivning

Webbshoppen är i dagsläget svår att lita på. Den visar ofta samma produkter flera gånger fast med olika pris. Den låser sig vid åtskilliga tillfällen, den ända lösningen för detta idag är att starta om webbservern. Kunddatabasen innehåller felaktiga användare. Produktdatabasen är rörig, datan är redundant och svår att tyda. Anställda får idag mycket skräp-e-post från webbshoppen vilket har skapat problem med webbshoppen servrar och även andra servrar inom företaget.

Bakgrund

Abelix vill gå över från postorderförsäljning till renodlad e-handel. Målet är att 80% av deras e-handel ska ske via deras webbshopp. Inom företaget står e-handel för 30% av omsättningen vilken motsvarar totalt 18 miljoner kronor. Antalet beställningar via webbshoppen har fördubblas varje år sedan ett par år tillbaka. I dagsläget hittar kunder produktutbud via papperskatalog eller digital katalog via e-post. Webshoppen som är i drift just nu är utvecklad av Nicolas som även har varit ansvarig för att uppdatera produktdatabasen och dokumentera instruktioner kring detta. Tanken nu är att Abelix vill satsa mer på en ny webbshopp och inser att detta kommer kräva mer fokus på IT-säkerhet.

Område

Webbshopp, produktdatabas, kunddatabas, serverdrift, e-postskydd.

Inblandad teknik/utrustning

Webbapplikation, webbserver, Paypal, CMS, kommersiella verktyg, affärssystem.

Iblandad personal

VD, chefer, ansvariga tekniker, Nicolas.

Vem äger problemet

VD äger problemet tillsammans med de 20-talet anställda på Abelix AB.

Konsekvens

Eftersom samma produkter visas flera gånger fast med olika pris kan kunder råka beställa fel produkter och kräva pengarna tillbaka, de blir dessutom missnöjda och det finns risk att de vänder sig till konkurrenter för att köpa varor hos dem istället. Att både kunddatabas och produktdatabas innehåller felaktig data kan innebära flera sårbarheter som kan orsaka att webbshoppen inte kommer fungera som det är tänkt. Om webbshoppen inte fungerar på korrekt sätt så orsakar även det tekniska problem för kunder men också för anställd personal på Abelix. Skräp-e-post till anställda kan orsaka massvis problem när det gäller säkerhet, redan idag har vi sett att servrar har hängt sig och slutat fungera på grund av ett skadligt e-postmeddelande som en anställd skickade vidare till alla anställda på företaget.

Riskbedömning

I detta fallet har riskbedömning skett genom att baserat på tidigare erfarenheter och statistiska underlag identifiera och sedan uppskatta risker som kan inträffa. Risker har värderats baserat på dess sannolikhet att de inträffar och på påverkan de kan innebära.

Förslag på hur riskerna ska hanteras

Vid nästa del i detta dokumentet beskrivs rekommendationer på hur alla dessa identifierade risker ska hanteras i form av en åtgärdsplan. Åtgärdsplanen kommer säkra de sårbarheter som hittats under riskanalysen.

Uppgift 2 (30 p)

Åtgärdsplan

I denna delen kommer det föreslås ändringar av webbapplikationen som kommer ge Abelix AB en tillräcklig säkerhetsnivå under det kommande året.

- Åtgärda att webbshoppen visar samma produkter flera gånger fast med olika pris genom att hämta produkter direkt från affärssystemets databas för att sedan lägga in dem i produktdatabasen automatiskt. Detta borde ändras för att se till att kunder inte råkar köpa fel produkter, också för att underlätta för personal som uppdaterar produktdatabasen.
- Åtgärda att Nicolas tappar bort sina lösenord till administrationsprogrammet för databas genom att ge honom något typ av verktyg som hanterar löserord(t.ex. 1Password). Detta borde ändras för att se till att Nicolas kan utföra sitt arbete ordentligt och underhålla webbshoppen så gott som det går.
- Åtgärda att webbshoppen låser sig genom att antingen införskaffa nya servar som kan hantera webbshoppens trafik o.s.v. eller genom att konfigurera servarna att starta om sig själva regelbundet. Detta borde ändras för att se till att webbshoppen hela tiden är brukbar för kunderna.
- Åtgärda att kunddatabasen innehåller icke-verkliga kunder genom att kräva mer information vid registreringstillfället som intygar att kunden är en riktig person som är en seriös kund. Detta borde ändras för att se till att kunddatabasen innehåller bra data som är användbar för företaget och dessutom inte kan orsaka skada i databasen.
- Åtgärda att anställda utsätts för skräp-e-post genom att implementera ett bättre skydd i inkorgarna på e-posten eller genom att helt enkelt inte ge ut anställdas e-postaddresser utan istället ha en support-e-post som inte lika lätt sprider vidare skadliga e-post inom företaget. Detta borde ändras för att se till att inte skadliga e-post sprids in i företagets system orsakar skada.
- Åtgärda att inbrott i server-rum kan inträffa genom att se till att alltid låsa server-rummen och alternativt införskaffa fler servrar som kan placeras på annan ort som reserv. Detta borde ändras för att se till att datan som affärssystem och webbshoppen hanterar alltid är säkrad från fysiska hot.
- Åtgärda planen för implementation av inloggningsfunktion genom att istället för att anlita VDs släktings dotter istället anlita en professionell webbutvecklare. Detta borde ändras för att förebygga säkerhethål i inloggningsfunktionen som kan skada webbshoppen allvarligt i framtiden.
- Åtgärda den grundläggande säkerheten för formulär på webbshopen genom att implementera enkla skydd mot SQL-injection och cross-site-scripting. Detta borde ändras för att se till att webbshoppen inte blir sårbar för de allra vanligaste attackerna som sker på webben idag.
- Åtgärda bristen av kompetens inom företaget genom att anställa fler personer som Nicolas med IT-kompetens. Detta borde ändras för att se till att företaget alltid har någon internt på plats som kan rycka in ifall problem uppstår, det kommer även underlätta underhåll av databaser och serverdrift o.s.v.
- Åtgärda det dåliga skyddet av känsligt information om företaget genom att införa standardprinciper som hjälper anställda på företaget att t.ex. skydda sina inloggningsuppgifter och annan information som inte får komma ut till allmänheten. Detta borde ändras för att se till att företaget är skyddat mot informationsläckor till externa personer.

Om alla dessa föreslagna åtgärder utförs så kommer inte bara webbapplikationens utan även företagets generella IT-säkerhet hålla en tillräckligt hög säkerhetsnivå det kommande året.

Uppgift 3 (30 p)

Kravspecifikation

Nedan beskrivs en kravspecifikation för Abelix nya webbshopp som ska byggas på ett professionellt sätt med hjälp av kommersiella verktyg.

- Webbshoppen ska byggas med det kommersiella CMS-verktyget Drupal.

  Det går att verifiera kravet genom att kontrollera om webbshoppen är byggt i Drupal.

- Webbshoppen ska erbjuda kortbetalning med hjälp av betalningstjänsten Paypal.

  Det går att verifiera kravet genom att kontrollera om webbshoppen erbjuder kortbetalning via Paypal.

- Webbshoppen ska ha ett skydd mot SQL-injections och cross-site-scripting (Stuttard & Pinto, 2011; Sullivan & Liu, 2012).

  Det går att verifiera kravet genom att kontrollera ifall webbshoppen kan stå emot SQL-injections och cross-site-scripting.

- Webbshoppen ska ha en filter som stoppar bottar från att skicka spam-e-post till företagets anställda.

  Det går att verifiera kravet genom att kontrollera antalet spam-e-post som de anställda får in i sina inkorgar.

- Webbshoppen ska ha en utförlig dokumentation som beskriver hur IT-ansvariga på företaget kan underhålla webbshoppen.

  Det går att verifiera kravet genom att kontrollera om det finns en dokumentation och ifall den hjälper det IT-ansvariga på företaget att underhålla webbshoppen.

- Webbshoppens mjukvara ska vara uppdaterad till senaste versionen (Sullivan & Liu, 2012).

  Det går att verifiera kravet genom att kontrollera att webbshoppens CMS Drupal är uppdaterat till den senaste versionen.

- Webbshoppen ska ha en funktion som kräver att alla användare(kunder, anställda, IT-ansvariga) ska uppdatera sina inloggningsuppgifter två gånger om året.

  Det går att verifiera kravet genom att kontrollera ifall alla användare får notifikationer två gånger per år om att de måste uppdatera sina inloggningsuppgifter

- Webbshoppens produktdatabas ska vara kopplad till företagets affärssystem så att produktdatabasen uppdateras automatiskt.

  Det går att verifiera kravet genom att kontrollera ifall webbshoppens produktdatabas är kopplad till företagets affärssystem, och genom att kontrollera att produkterna i produktdatabasen är samma som de produkter som finns i affärssystemet.

- Webbshoppen ska stänga av alla Drupals funktioner som inte används, t.ex. DNS-servrar och fjärradmin-verktyg (Sullivan & Liu, 2012).

  Det går att verifiera kravet genom att kontrollera ifall alla funktioner i Drupal som inte används är avstängda.

- Webbshoppens server ska ha en brandvägg aktiverad och anti-virusprogram installerade (Stuttard & Pinto, 2011).

  Det går att verifiera kravet genom att kontrollera ifall det finns en brandvägg aktiverad och anti-virusprogram installerade på servern som webbshoppen ligger på.

- Webbshoppen ska kryptera all data som skickas mellan client och servern (Stuttard & Pinto, 2011).

  Det går att verifiera kravet genom att kontrollera ifall datan krypteras innan den skickas in i databasen på servern.

- Webbshoppens loggfiler ska säkerhetskopieras och sparas på flera olika separata platser på servern bakom brandväggen (Stuttard & Pinto, 2011).

  Det går att verifiera kravet genom att kontrollera ifall det finns flera kopior av loggfilerna på olika platser på servern.

- Webbshoppens kommunikationskanaler ska vara krypterade med SSL (Stuttard & Pinto, 2011).

  Det går att verifiera kravet genom att kontrollera att webbshoppen har SSL-kryptering installerat.

- Webbshoppen ska dölja debug- och fel-koder för obehöriga användare (Stuttard & Pinto, 2011).

  Det går att verifiera kravet genom att kontrollera att ingen debug- eller fel-koder visas för någon annan användare än admin.

- Webbshoppen ska stänga av både FTP, SMTP, och directory browsing (Stuttard & Pinto, 2011).

  Det går att verifiera kravet genom att kontrollera ifall FTP, SMTP, och directory browsing är avstängt på servern.

Referenslista

Stuttard, D., Pinto, M. (2011). *The Web Applications Hacker's Handbook: Finding and Exploiting Security Flaws. Indianapolis*: Wiley Publishing.

Shems, M. (2011). *Web Application Security For Dummies.* Chichester: John Wiley & Sons, Ltd.

Sullivan, B., Liu, V. (2012). *Web Application Security: A Beginner's Guide.* New York: The McGraw-Hill Education.

Tonnquist, B. (2012). *Projektledning*. Stockholm: Sanoma Utbildning AB.