Vitbok om säkerhetsfunktionalitet i deaddrop

Detta dokument är en kort beskrivning av säkerheten och säkerhetsslösningarna som används i deaddrop. Målet med dokumentet är att ge läsaren en bättre förståelse för säkerheten i lösningen och för att förmedla hur säkerhet är en central funktion och kvalitetsbegrepp under utvecklingen av produkten.

Säker design

Bra säkerhet har varit ett grundläggande designkriteria från början, vilket för att det genomsyrar hela sättet som lösningen byggts, både på konceptnivå men också i olika designval.

En grundläggande designkoncept som använts genomgående är ”defense in depth”, där flera säkerhetsbarriärer existerar för att komplettera och överlappa varandra.

En annat grundläggande säkerhetsprincip som genomsyrar lösningen är ”keep it simple”. Därför används till exempel ingen databas i severdelen. Detta får också säkerhetsmässiga fördelar då hela attackklasser eliminseras, tex attacker mot SQL eller databaskomponenten.

Säkra defaults

I alla fall där det finns olika valmöjligheter för standardinställningar, så har används säkra standardinställningar.

Användarsäkerhet

Separation av kontoinfo

Användarnamn och länk till en nedladdningssida där deaddrop-filer hämtas skickas via ett mail till mottagaren. Lösenord skickas via SMS, telefonmeddelanden till användaren mobiltelefon. På så sätt försvåras möjligheten för någon att fånga upp komplett information för att komma åt konto.

SSO, single-sign-on

Deaddrop har möjligheten att använda sig av integrering mot ett Windows AD för vissa eller alla användare. Detta möjliggör att dessa användare får en SignleSignOn-lösning där deras AD-konto ger en smidigare inloggning mot deaddrop. Åtkomsten till deaddrop kan sedan styras via grupper i AD. Kopplingen mot AD sker krypterat via LDAPS[1].

Lösenordpolicy

Det går att styra lösnordspolicyn i deaddrop. På så sätt ges administratören möjlighet att kräva viss lösenordskvalitet. Via administrationsgränssnittet så bestäms komplexiteten på lösenorden. Detta gäller för både de automatgenererade engångslösenorden som systemet skickar via SMS såväl som kontrollen av de lösenord som en användare själv kan sätta.

Automatutloggning

Efter inaktivitet, så blir en användare automatiskt utloggad från sitt deaddropkonto. Tiden för inaktivitet är inställbar av administratören.

Säkerhet i överföring

TLS-kryptering

All data mellan webbklient och server sker krypterat med hjälp av TLS[2]. Uppsättning och konfiguration av TLS är restriktivt satt, så att

---

1 https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

2 https://en.wikipedia.org/wiki/Transport_Layer_Security

enbart starka kryptoalgoritmer och den senaste varianten av TLS-protokollet används.

http-säkerhet

Flera headers i överförd protokollinformation sätts av server för att kontrollera hur webbklienten hanterar sessioner och överförd information. Exempelvis används HSTS[3], ett sätt att tvinga en användare och instruera dess webbläsare att alltid ansluta via HTTPS istället för HTTP.

En annan skyddsmekanism som används på webbnivån är såkallad CSRF[4]. Detta är ett skydd mot att återanvända eller missbruka sessioner och länkar.

För att inte läcka information till webbläsaren så använder sig lösningen inte av webbkakor (cookies).

Det går att få ytterliggare säkerhet i lösningen genom att använda s.k. certificate pinning via HPKP[5].

En viktig webb och http-säkerhetsmekanism är CSP[6], s.k. content security policy. vilket är ett sätt att styra webblienten i hur den skall tillåta laddning av HTML och innehåll. Genom att från deaddrop instruera klienten att vara extremt strikt i hur webbläsaren skall ta emot innehåll, så kan webbläsaren begränsas till att inte tillåta tredjepartsladdning av material eller sättet som skript inkluderas i innehåll. CSP är ett starkt skydd mot att information hämtas från en hackad eller illasinnad tredjepartsleverantör av innehåll, exempelvis bildmaterial eller javaskriptsfunktioner.

För att hantera problemet med osäkert tredjepartsinnehåll, så är deaddrop byggt så att allt material för att bygga webbsidor hämtas från deaddropservern, även om det är standard javascripts-bibliotek. Detta för att få kontroll över versioner av biblioteken som blivit utvald och säkerhetskontrollerade.

Serversidessäkerhet

Säker installation

Inga standardlösenord eller säkerhetsinformation såsom digitala certifikat är förskapade från leverantören. Allt sådan genereras automatiskt och är unikt per installation.

Säker administration

Administrationen av deaddrop är separerad från användningen av deaddrop till den grad att det är olika webbservrar som kör på olika portar. Detta gör att det är enklare att styra i brandväggar och på nätnivå vilken eller vilka som skall få åtkomst till administrationssidorna.

Adminsitrationen sker via olika roller som har olika behörighetsnivåer. Vissa administratörsroller ges åtkomst för enklare löpande administration, exempelvis skapa användare eller byta lösenord.

---

3 https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

4 https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet

5 https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning

6 https://en.wikipedia.org/wiki/Content_Security_Policy

Säker förvaltning

Lösningen använder sig av en mekanism för automatuppdateringar. På så sätt hämtas nya programpaket och installeras i bakgrunden. Genom detta så får man en s.k. evergreenlösning där systemet alltid kör de senaste versionen av operativsystem och använda programpaket.

Deaddropsystemet kontrollerar att alla paket är elektroniskt signerade av utgivarna innan något paket installeras. Detta gäller för såväl operativsystemet som för deaddrop-programvaran.

Alla uppdateringar hämtas från en betrodd uppdateringsserver, dvs både operativsystem och deaddrop-paket. Detta förenklar för deaddropkunder i det att enbart en brandväggsöppning behövs.

Beprövad inloggningsteknik

Bakom kulisserna i kommunikationen mellan webbklient och server så används s.k. basic auth, vilket är ett standardiserat och väl uttestat sätt att autentisera användare.

Egen server

Deaddrop är inte en tjänst som köps via nätet. Det är en server med programvara som installeras fysiskt eller virtuellt på en plats där licenstagaren ser passa bäst. På så sätt ges maximal kontroll över åtkomst till informationen och system, vilken juristiktion som gäller för information och system, med mera.

Indatakontroll

Indatakontroll sker på flera ställen i deaddrop, både i webbklienten och på serversidan. Klientsideskontrollerna fungerar som hjälp för användaren att förstå vilka fält som tillåter vilken indata på serversidan. Serversides-kontrollerna är de som används för att skapa säkerhet och kontrollera att rätt information, utan skadliga eller farliga tecken, tas emot till servern.

Tidsbegränsningar

All uppladdad information, som filer, har ett begränsad livslängd på servern. Tidsgränsen går att sätta mellan 1 timme och 14 dagar. Efter att tidsgränsen uppnåtts så raderas filer automatiskt.

På ett liknande sätt som filer är tidsbegränsade så går det att skapa temporära konton. Det är ett sätt att delegera användarskapandet. Med rätt rättigheter så kan en deaddropanvändare skapa andra, temporära, användare. Detta för att kunna kommunicera filer fram och tillbaka. Dessa användare ges ett livslängd på mellan 1 timme och 14 dagar.

Härdning av operativsystemet

Alla deaddrop-programpaketen installeras på en härdad version av Linux.

Uppsäkringen av operativsystemet följer leverantören RedHats riktlinjer, men går även längre för att skapa extra säkerhet.

Härdning av nyckel-komponenter

De nyckelkomponenter som används i deaddrop, såsom webbservrar, är uppsatta på ett restriktivt sätt för att förhindra manipulation och för att minimera attackytor.

Sandbox och nedlåsning

Deaddrop är uppbyggt med ett antal små, isolerade och specialiserade program. Vart och ett av dessa program används för enbart

en typ av funktion på serversidan. Detta för att isolera och hantera de olika funktionerna så restriktivt som möjligt. Detta följer också av principen ”keep it simple”, vilket möjliggör att varje program hålls enkelt och överskådligt.

För att låsa ned de skript och den exekveringsmiljö som finns på serversidan så används den avancerade tekniken SELinux[7]. Med hjälp av SELinux skapas systemöverskridande säkerhetsinställningar som ligger utanför de exekverande progrogrammen. Säkerhetsinställningarna skapar ett till lager av restriktioner och kontroll över vad ett exekverande program kan få åtkomst till och vad det kan göra. Varje program och tjänst i deaddrop är nedlåst med separata SELinux-policies som avgränsar de olika programmens funktionalitet. På så sätt så kan varje enskilt program hållas extremt restriktivt. Exempelvis så tillåts ett program som skall uppdatera kontaktboken att enbart uppdatera kontaktboksdata. Det tillåts inte att läsa delar av systemet där uppladdade filer sparas.

Ännu bättre sandboxstöd

Seccomp är en mekanism i Linux för att låsa ned ett programs tillgång till underliggande systemanrop. Genom att programmet ges en begränsad åtkomst till systemanrop så kan ett program styras och kontrolleras på detaljnivå. Exempelvis kan ett program blockeras från att starta nya program eller skriva till filer. Seccomp används av deaddrop för att låsa ned de olika programmen som exekverar på serversidan.

[7] https://en.wikipedia.org/wiki/Security-Enhanced_Linux

Loggning

Det underliggande operativsystemet är uppsatt att logga extensivt. Auditd

Alla moduler i deaddrop loggar användning.

Deaddrop stödjer syslog-protokollet, vilket är defactostandard bland olika system. Detta möjliggör att loggar kan skickas till loggservrar via nätverket.

Granskning och kontroll

Kunder och användare ges möjlighet till säkerhetsgranskningar av lösningen. Kunder kan, efter tecknande av NDA, få tillgång till säkerhetsgranskningar som tredjepartsorganisationer utfört för deaddropanvändares räkning.

Källkod är tillgänglig för källkodsgranskning.

Säkerhetskopiering

Systemet har inbyggd möjlighet till säkerhetskopiering. Av säkerhetsskäl så omfattar säkerhetskopieringen bara metadata och systeminställningar, inte uppladdade filer.

Framtida säkerhets-förbättringar

Dessa säkerhetsförbättringar är funktioner som det för närvarande arbetas med i utvecklingen av deaddrop.

Federerad autentisering, SAML

Genom att använda sig av SAML[8], så uppnås möjlighet att använda sig av federerade lösningar för autentisering. Med en s.k. iDP,

[8] https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

identity provider, så kan tredjepartstjänster för identitetskontroller användas. Detta möjliggör att använda andra typer av autentiseringsmekanismer, såsom tokens, i deaddrop.

Grupphantering

Med den nya grupphanteringsfunktionen som byggs in i deaddrop, så ges användaren bättre kontroll när utskick av filer sker till multipla mottagare.