IT-Säkerhetspolicy

2018-01-25

Rackfish AB

DOKUMENTNAMN:	IT-Säkehetspolicy	SKAPAT DEN:	2009-09-14
TYP AV DOKUMENT:	Policy	SENAST ÄNDRAT DEN:	2018-04-17
FILNAMN:	IT-Säkerhetspolicy	VERSION:	2018 v1
DOKUMENTÄGARE:	Rackfish CTO		

Behörighetskontroll

Allmänt
Varje användare tilldelas en personlig användaridentitet, i det flesta system baserade på e-postadress, och starka lösenord. För de system som så stödjer det har Rackfish en centralt hanterad "directory-tjänst" för alla användare.

Inloggningsförfarande bör endast vara möjligt över krypterade anslutningar.

I den mån så är möjligt skall utloggning ur system ske automatiskt.

Streamio:
Varje konto tilldelas en "huvudanvändare" som kan och skall styra vilka användare som har tillgång till kontot. Samma användare kan ha tillgång till ett eller flera konton och olika konton inom en organisation kan ha olika huvudanvändare. Det är inte rekommenderat att använda gemensamma funktionskonton eftersom det då inte går att se vilken användare som gjort vilka åtgärder.

Lagring och säkerhetskopiering

Allmänt
System för vilka Rackfish ansvarar, exempelvis gemensamma system såsom DNS, delade system såsom Webbhotellstjänster, interna system såsom debiteringssystem görs regelbunden säkerhetskopiering till vårt sekundära datacenter som är geografiskt åtskilt från vårt primära datacenter.

IaaS-tjänster
För infrastrukturtjänster som levereras som en service till kund, såsom exempelvis servrar, utförs säkerhetskopiering av data enligt avtal. Om inget avtalats sker ingen säkerhetskopiering.

Streamio
För Streamio säkerhetskopieras det gemensamma datat, såsom konton, själva systemet och metadata regelbundet. Media som laddats upp till tjänsten har tredubbel redundans, dvs är lagrat på tre skilda lagringsenheter, vilket ger en god säkerhet för eventuella datafel eller hårdvarufel. Media backas i övrigt inte upp, utan en raderad fil raderas ur systemet direkt.

Datakommunikation

Allmänt
Vi arbetar aktivt med att kryptera all kommunikation, både internt och externt. Vi arbetar med olika nivåer av skydd för att hantera intrång, från nätverksbaserade DDOS skydd till, brandväggar, Intrusion Detection Systems, Web application firewalls etc.

IaaS och Delade tjänster
Rackfish rekommenderar att man använder kryptering på alla servertjänster som är öppna på en server, liksom alla webbplatser på delade system. Detta är dock kunds ansvar att tillse, då det kan leda till problem och kräva åtgärder i applikationer om man slår på kryptering tvingande.

Streamio
Streamio applikationen är krypterad, medan publicerad media är åtkomlig både krypterat och okrypterat.

Loggning

Allmänt
Rackfish loggar händelser i sina system, innefattande bland annat access, nätverkstrafik och inloggning. Detta sker bland annat för att kunna hantera debitering (vilket kräver att loggarna sparas en längre tid som underlag till debiteringen), felsökning och spårbarhet vid säkerhetshändelser.

Loggar övervakas och analyseras.

Loggning sker på flera nivåer, i nätverksutrustning, olika brandväggs- och andra säkerhetssystem samt på servernivå (exempelvis webbserver och databaser). Loggning sker även på Rackfish interna och gemensamma system såsom kontrollpaneler, DNS och liknande. Loggar skall alltid raderas inom 24 månader.

Delade tjänster
För delade tjänster följer vi Rackfish policy om att radera loggar senast inom 24 månader.

IaaS
För Infrastrukturtjänster är kund ansvarig att tillse att de operativsystem och tjänster som installeras har korrekt hantering av loggar. Om tjänsten är Managed by Rackfish så är det kunds ansvar att begära att loggning ställs in i enlighet med den egna policyn.

Streamio
Streamios loggningspolicy följer Rackfish allmänna loggning.

Utplåning

Lagringsmedia som tas ur drift förstörs så att uppgifter inte kan återskapas.

Uppdatering

Allmänt

Rackfish har en strikt policy för uppdatering där vi prioriterar säkerhetsuppdateringar mycket högt för att minimera luckan när ett säkerhetshål kan utgöra en angreppsyta. Detta skall, där så är möjligt, ske med automatik.

IaaS

För infrastrukturtjänster, såsom servrar, ansvarar kund för att utrustningen hålls fullt uppdaterad och att kända säkerhetshål stoppas. Rackfish levererar normalt servrar med automatiska uppdateringar påslaget. Om kund begär eller själv ställer in server för att inte följa dessa uppdateringar ansvarar kund för följderna av detta, vilket kan innebära att utrustning stängs ner utan ersättning till kund samt kostnader för det arbete som utförs av Rackfish, i händelse av eller till följd av detta.

Utbildning

Rackfish personal skall arbeta aktivt med alla säkerhetsfrågor och kontinuerligt uppdatera rutiner och instruktioner för detta. Nyheter, såsom nya sårbarheter, skall omedelbart delas med all berörd personal så att samtlig personal är fullt uppdaterad. Vidareutbildning hålls kontinuerligt där all berörd personal informeras och tränas i hantering av säkerhet.

Fysisk säkerhet

Rackfish skall bara använda datahallar som övervakas dygnet runt med personal tillgänglig.

Datahallar skall vara utrustade med brandskydd och klimatsystem. I hallar för primär drift skall dessa system vara fullt redundanta.

Anslutningar skall vara redundanta och ha tillfredställande överkapacitet för att hantera trafiktoppar så att användares tillgång till tjänsterna kan säkerställas.

Endast godkänd personal skall vara ha tillträde till datahall.

Alla lösningar; tekniska, fysiska såväl som funktionsmässiga, skall, där så är tekniskt och ekonomiskt försvarbart, vara fullt redundanta.

Servrar och nätverk skall skyddas av system för överbelastningsattacker, intrång och annan otillåten åtkomst genom tekniker som brandväggar, DOS-mitigering, IDS, ip-övervakning och blockering, externa filter med mera. Dessa lösningar övervakas proaktivt.

Kunskapen om hur säkerhetssystemen är konfigurerade är en affärshemlighet som endast är känd av de personer som aktivt arbetar med detta. Det är inte tillåtet att lämna ut specifik information om systemens uppbyggnad utan godkännande av CTO.