Incidentrapport

Driftstörningar i Skolfederation 5 Mars 2018

Stockholm 2018-03-05

Johnny Pihl
Chef Infrastruktur

Innehållsförteckning

1 Sammanfattning av incidenten

På morgonen den 5 mars 2018 meddelar kundtjänst att de fått in samtal från medlemmar i skolfederation som har hört av sig angående ett TLS-certifikat som har löpt ut (ogiltigt datum) för fed.skolfederation.se. Detta medför att certifikatkedjan för fed.skolfederation.se är bruten och därmed inte går att validera.

IIS IT-tekniker tar sig an incidenten och uppfattar snabbt vad som är fel och hur problemet ska lösas. Teknikern beställer ett nytt certifikat från Comodo och byter ut det gamla i webbservern, teknikern verifierar sedan från sin klient att allt ser bra ut och det anses att ärendet är löst.

Någon timme senare visar det sig dock att certifikatkedjan inte validerar hela vägen, orsaken är att certifikatleverantören Comodo uppdaterat ett så kallat intermediate certifikat, alltså ett mellanliggande certifikat, vilket inte blivit uppdaterat på webbservern.

Teknikern lägger till även detta certifikat i webbservern och validerar denna gång via ett verktyg som finns på ssllabs.com och konstaterar att hela kedjan validerar korrekt.

2 Driftstörning distribution

2.1 Beskrivning av incidenten

Händelseförlopp rapporterad av Teknik:

08:55	*Certifikatet för fed.skolfederation.se löpte ut vid natten till den 5 mars. Påverkan för samtliga kunder som vill hämta metadata* *Vi har missats att förnya det i tid och fick nu snabbt förnya på morgonen idag och såg efter det OK ut.*
10.00	*Vid förnyandet så missades vi att CA-cert var bundlat med server-certet i samma fil. Vilket innebar att webbläsaren tyckte detta var OK, fast kedjan egentligen ej var OK för vissa klienter som verifierade hela kedjan.*
	Nytt intermediate-certifikat genererades. Detta las sedan in i samma CA-Certifikat som server-certet.
12.30	*Certifkatkedjan valideras mot ssllabs.com*

2.2 Åtgärder

Certifikat uppdaterade och kedjan validerades.

3 Krishantering

Vd, säkerhetschef, affärsområdeschef, Skolfederations tjänsteägare och IT-chef informerades om ärendet.

4 Konsekvenser

Medlemmar i Skolfederation kunde inte hämta metadata från fed.skolfederation.se.

4.1 Erfarenheter

Behovet av att hantera certifikat bättre är uppenbart. Rutiner och arbetssätt på IT-avdelningen behöver ses över.

5 Vidtagna åtgärder och fortsatt arbete

1. Säkerställa larm i övervakning för detta certifikat där giltighetstid framgår.
2. Gå igenom beredskapsrutiner och förtydliga eller komplettera dessa vid behov – Möte inbokat
3. Se över larm generellt för verksamhetskritiska tjänster
4. Ta fram förslag till med automatiserad lösning för att förhindra handhavandefel.

6 Slutsatser

Med ovan *vidtagna åtgärder och fortsatt arbete* samt bättre, tydligare, rutiner och dokumentation har IT-avdelningen för avsikt att kunna förhindra liknande situationer framöver.