NR 11/2017

Dato: 03.11.17

Til: Bankene
Att: IT-ansvarlig, Sikkerhetsansvarlig
Kontaktperson i Bits: Erik Bergersen
Arkivref: 17-884-1

Rundskriv fra Bits omfatter hovedsakelig informasjon fra Bits knyttet til regelverk, utfyllende regler og krav, standarder og anbefalinger. Rundskrivet stiles til det fagmiljø som antas å ha mest nytte av informasjonen. Det forutsettes at mottaker av rundskriv fra Bits foretar den nødvendige interne distribusjon i egen organisasjon.

Anbefalinger til sikkerhetstiltak for å bedre sikkerheten for e-post og navnesystemer for domenenavn

Med dette rundskrivet vil Bits informere om anbefalinger til løsninger og standarder som er utviklet for å beskytte bedrifter mot kjente svakheter i løsninger for kommunikasjon over Internett. Teknologiene er i stor grad knyttet til e-post, men omfatter også navnesystemer (DNS - Domain Name System).

Trusselbildet

Flere av standardene nevnt i dette rundskrivet er generelle løsninger/standarder som er utarbeidet for å sikre at e-post ikke kan forfalskes. For banknæringen er det spesielt viktig å beskytte seg imot phishing da det er en utbredt metode som benyttes for å tilegne seg kunders kortinformasjon eller innloggingsinformasjon til nettbanker. Andre tiltak som adresseres gjennom anbefalingene er beskyttelse av aktørene mot forfalskning av DNS-svar, hvor en svindler kan ha modifisert svaret. Løsningene kan også beskytte mot sikkerhets- og tillitsbrudd hos tillitsankrene på Internett. Flere av truslene og løsningene har blitt omtalt i norske medier de siste året. NRK har skrevet en rekke artikler rundt bruken av standardene for å sikre mot forfalskning av e-post[1]. Nettavisen Digi.no informerte tidligere i år om at mange nettsteder måtte skaffe nye sertifikater grunnet manglende tillit til Symantec sin prosess for å utstede sertifikater[2]. Bits anbefaler derfor at bankene implementerer følgende tre løsninger for å heve sikkerheten.

[1] https://www.nrk.no/dokumentar/stopper-falske-nettbanker-nesten-daglig-1.13285516
[2] https://www.digi.no/artikler/mengder-av-nettsteder-ma-trolig-skaffe-seg-nye-sertifikater/378633

1) Sikker kommunikasjon mellom e-postservere - Tvungen TLS

TLS (Transport Layer Security) kan benyttes for å sikre kommunikasjonen mellom to e-postservere over Internett. Banknæringen utveksler i dag personopplysninger på e-post. Kryptering av denne informasjonen er påkrevd når den utveksles over Internett. Bits har derfor utarbeidet en kravspesifikasjon for bruk av tvungen TLS mellom aktører som melder inn sine domener til Bits (vedlegg 1). Formålet med en standardisert løsning for TLS fremfor bilaterale avtaler er å bidra til en forenklet administrasjon og implementering der banken forholder seg til en liste publisert av Bits.

Finans Norge informerte om tvungen TLS i rundskriv 22/2017. Hovedstyret i Finans Norge ble informert om TLS-ordning i et møte 7. september 2017, og sluttet seg til oppfordringen om å knytte seg til løsningen. Bits er kjent med at mange banker allerede har implementert tvungen TLS.

2) Tiltak mot forfalskning av e-post – SPF, DKIM og DMARC

Phishing der avsenderadressen på en e-post er forfalsket er en gjentagende utfordring. Bits anbefaler i vedlegg 2 flere standarder for å forhindre at avsender utgir seg for å være en annen enn de faktisk er i e-postkommunikasjon:

- SPF (Sender Policy Framework) er en løsning som kontrollerer at e-post kommer fra en sender som er autorisert av domenets administrator.
- DKIM (DomainKeys Identified Mail) sender med en digital signatur av e-posten, som e-postmottaker kan verifisere ved å benytte den offentlige nøkkelen til avsender.
- DMARC (Domain-based Message Authentication, Reporting and Conformance) er bygget på toppen av SPF og DKIM, og retter svakheter ved standardene, i tillegg til at den tilrettelegger for blant annet rapportering.

Bits vet at flere av bankene har implementert standardene og at flere for tiden tester ut bruken av DMARC. Bits anbefaler at alle tre standardene implementeres for å hindre at uvedkommende sender forfalskede e-poster fra bankenes e-postadresser.

Bits publiserte i mars et dokument om forebygging av direktørsvindel (vedlegg 3). Et av rådene i dette dokumentet var å benytte løsningene som er nevnt ovenfor. DMARC vil ikke direkte hindre direktørsvindel, men vil beskytte mot forfalskning, phishing og spam som ofte er en av angrepsmåtene i forbindelse med direktørsvindel.

3) Tiltak mot forfalskning av kommunikasjon – DNSSEC og DANE

DNSSEC (Domain Name System Security Extensions) og DANE (DNS-based Authentication of Named Entities) er to standarder som har til hensikt å beskytte mot svakheter i viktige protokoller for kommunikasjon over internett. Se vedlegg 4. DNSSEC beskytter integriteten til DNS-svar og autentiserer at det kommer fra en tiltrodd kilde. DANE vil blant annet beskytte mot sikkerhetsbrudd hos sertifikatutstedere.

Svakhetene i DNS har så langt ikke blitt utnyttet i stor skala, men det må antas at dette vil bli utnyttet i fremtiden. Bits anbefaler derfor bankene om å implementere DNSSEC og DANE som et proaktivt tiltak.

Anbefaling

Gjennom dette rundskrivet og vedleggene presenterer vi en rekke teknologier bankene bør implementere for å øke sikkerheten. Samlet sett står banknæringen sterkere hvis alle bidrar til økt sikkerhet, fordi det gir økt tillit fra samfunnet til den digitale infrastrukturen bankene benytter i dagens prosesser.

Vi ber bankene vurdere de foreslåtte løsningene, og gi Bits en tilbakemelding på hvordan de vurderer de ulike teknologiene, og når banken eventuelt vil implementere løsningene.

Bits er behjelpelig med ytterligere informasjon, ta evt. kontakt med Erik.Bergersen@Bits.no

Med vennlig hilsen
Bits AS

Vedlegg:

1. Krav til Tvungen TLS
2. SPF, DKIM og DMARC - Autentisering av e-post
3. Forebygging av Direktørsvindel (CEO-fraud)
4. DNSSEC og DANE – Sikring mot forfalskning av kommunikasjon