

2014/01/21

EPR05/2014

www.enisa.europa.eu

EU:s IT-säkerhetsmyndighet ENISA kräver säkrare e-banking samt e-betalningar: icke-replikerbara, engångskoder för e-identiteter behövs i den finansiella sektorn

Olika bankdosor, apparater, mobiltelefoner, e-signaturer, m.m. används för att autentisera våra e-identiteter online. Ändå har vissa finansiella institutioner fortfarande otillräckliga mekanismer för autentisering med tanke på riskerna menar EU:s myndighet ENISA i en ny studie. I rapporten analyseras aktuella e-finans bedrägerier och relaterar dem till de finansiella institutionernas autentiseringsmekanismer för kunderna. Rapporten understryker behovet av uppdaterade säkerhetsmekanismer, samt rekommenderar 10 metoder för ökad säkerhet.

Myndigheten har analyserat mer än 100 enkätsvar från handel-, e-banking och IT-säkerhetsexperter om elektronisk identifiering och verifiering metoder (eIDA- electronic IDentity and Authentication methods). E-finans- och e-betalningssystemen används dagligen av medborgare, kunder och företag. Dessutom har myndigheten identifierat risker och attackmönster för varje autentiseringsmekanism, inklusive "phishing" (dvs riktade, individuella attacker), ID-stölder, sessions- samt identitets-kidnappningar, m.m. för finansiella institutioner, handlare samt leverantörer av betalningstjänster.

Huvudrekommendationer

Som resultat har myndigheten tagit fram riktlinjer, bästa praxis samt rekommendationer för e-banking och internetbetalningar. Bland de viktigare rekommendationerna är:

- **1. Förbättra säkerheten inom e-finans**, vilket innebär att ekonomiska aktörer måste:
 - Göra riskanalys utifrån kundernas profil och storlek på institutionen,
 - Förbättra kundernas medvetenhet och kompetens,
 - Genomföra verifieringsmetoder anpassade till kundens beteendeprofiler och transaktioner parametrar (t.ex. destinationsland, belopp)
 - Tidigare upptäckt om kundernas enhet är attackerad genom registrering av olika enheter, testning, samt utvärdering av deras säkerhet. ("**Förutsätt att alla enheter är smittade**").
- **2. Förbättra säkerheten för e-finance applikationer och deras distributionskanaler till kunderna**: genom att uppmuntra till den traditionella "säkerhet vid design" verkligen genomförs. Man bör även ta hänsyn till förslaget till nytt [persondataskyddsdirektiv](#), samt använda pålitliga kanaler för när man installerar program i kundernas enhet.
- **3. Stötta en proportionell bedömning mellan valda metoder, deras robusthet och den aktuella identifierade risken** (t.ex. tillräckliga eIDA-metoder vid transaktionssammanhang, med fokus på användning av "2-faktors autentisering" -även för lågriskverksamhet (som t.ex. uttagsautomater har; ett kort och en PIN-kod).
- **4. Förbättra kunskap och beteendet hos både kunder och personal.**

För att sammanfatta; nuvarande eIDA-metoder inom den finansiella sektorn täcker idag inte flera risker. ECB och EU-kommissionen håller på att utveckla rekommendationer och bestämmelser i linje med ENISA-rapporten för att identifiera och ta fram verktyg för att minska finansiella förlusterna på grund av bedrägeri.

Den [verkställande direktören](#) för ENISA, professor Udo Helmbrecht, kommenterade: "*Den finansiella sektorn hanterar e- transaktioner för hundratals miljarder euro varje år. Därför är säkra e-identiteter och autentisering helt enkelt ett måste för ekonomin i Europa. De finansiella institutionerna bör använda säkerhet som ett konkurrensmedel och marknadsföringsverktyg. Med*

ENISA is a Centre of Expertise in Network and Information Security in Europe

Securing Europe's Information Society

The European Union Agency for Network and Information Security

2014/01/21

EPR05/2014
www.enisa.europa.eu

den här rapporten kan de ekonomiska aktörerna göra en kostnads- nyttoanalys av olika autentiseringsmetoder."

Hela [rapporten](#)

Bakgrund: Förslaget till EU-direktiv om [dataskydd](#), [betaltjänstdirektivet II](#), samt ECBs "[Rekommendationer om säkerheten vid internetbetalningar](#)"

För intervjuer: Ulf Bergström, kommunikationschef och talesman,
ulf.bergstrom@enisa.europa.eu, mobil : + 30 6948 460 143, Manel Medina , ENISA Expert ,
sta@enisa.europa.eu

Detta är en inofficiell översättning; den enda giltiga versionen är det engelska originalet.

ENISA is a Centre of Expertise in Network and Information Security in Europe

Securing Europe's Information Society

The European Union Agency for Network and Information Security