6. Lecke: Biztonság és adatvédelem az elektronikus kereskedelemben

Ahogyan a hagyományos kereskedelem esetén, úgy az elektronikus kereskedelemben is előfordulhatnak szándékos károkozások, amelyre a vállalkozásnak fel kell készülnie. A károkozás irányulhat a kereskedőre, de akár a potenciális felhasználóra (pl. bankkártya vagy más adatok megszerzése). Annak érdekében, hogy a vásárlók biztonságban tudják vásárlásaikat lebonyolítani, a vállalkozónak egy biztonságos felületet kell biztosítania a vásárlásokhoz.

6.1. Titkosítás

Az interneten terjedő információk áramlásához különböző szabványokat alakítottak ki, amelyek biztosítják az információ zavartalan áramlását. Ezeket hívjuk protokolloknak, ezek biztosítják a zavartalan kommunikációt az üzenetet küldő és fogadó fél között. Ennek legismertebb eszköze **a „HyperText Transfer Protocol", vagy közismertebb nevén a „HTTP"**. Ezzel akkor találkozhatunk, amikor a böngészőbe beírjuk a weboldal címét és a „www." előtt látjuk a protokoll megjelölését.

A gyakorlatban ezen a protokollon keresztül történik a kommunikáció, amelyet a rendszer a különböző eszközökön (router, hálózati csomópontok, szerverek) keresztül áramoltat. A problémát viszont az okozza, hogy **a HTTP nem titkosított**, így abban az esetben, ha a valaki rácsatlakozik az egyik hálózati csomópontra, akkor láthatja az általunk küldött adatokat. Ez például a bankkártya és egyéb személyes adatok vásárláskor történő megadása esetén különösen nagy veszéllyel jár a vevő számára. De ugyanúgy a webáruházat üzemeltető is féltheti adatait, hiszen a belépési felületen keresztül megadott felhasználóneve és jelszava szintén illetéktelenek tulajdonába kerülhet.

A titkosítást a gyakorlatban a Secure Sockets Layer (SSL) vagy Transport Layer Security (TSL) protokoll végzi, amely a meglévő HTTP protokoll felett egy titkosított HTTPS kommunikációt valósít meg. A HTTPS elnevezés végén az „S" betű a „secure", vagyis biztonságos elnevezésre utal. Így ha bárhol böngészünk és személyes adatot kell megadnunk, akkor figyeljünk arra, hogy a protokoll esetén a HTTPS felirat legyen. Ahhoz, hogy ez a biztonságos kommunikáció megvalósuljon, a webáruház adminisztrátorának egy ún. tanúsítványt (public key certificate) kell készítenie. A titkosítás során egy kétkulcsos titkosítás történik, amely esetén a „nyilvános kulcshoz" tartozik egy „titkos kulcs". A vállalkozás pedig a titkos kulcs segítségével tudja visszafejteni a vásárló által megadott információkat.

Jelen tananyag a Szegedi Tudományegyetemen készült az Európai Unió támogatásával. Projekt azonosító: EFOP-3.4.3-16-2016-00014

6.2. Támadások elleni védelem

Ahogyan a fizikai üzletek esetén is védenünk kell értékeinket, úgy az online környezetben fel kell készülnünk rosszindulatú támadásokra. Ezeket a támadásokat jellemzően hackerek vagy internetes vírusok okozzák. Mindkét támadás esetén a cél a weboldalunk gyenge pontjait kihasználni és úgy hozzáférni a weboldalhoz és a rajta tárolt adatokhoz.

A hackerek célja sok esetben a weboldal biztonsági rendszerének feltörése és a weboldal adatbázisához való hozzáférés vagy a weboldal módosítása. Tekintsük is át, hogy pontosan milyen pontjait tudják megtámadni a weboldalnak. A weboldal megtámadásának az egyik legelterjedtebb módja a szerver feltörése. Abban az esetben, ha saját magunk működtetjük a szervert, akkor folyamatosan karban kell tartanunk és megfelelő tűzfallal kell rendelkeznünk. Ha külső tárhelyszolgáltatótól béreljük a tárhelyt, akkor érdemes olyan szolgáltatót választani, amely jól ismert és garanciát vállal a szerverein futtatott weboldalak védelméért. Kisebb vállalkozások gyakran nem tudják megfizetni a magasan képzett szakembereket, így sok esetben praktikus megoldás lehet külső tárhelyszolgáltató megbízása a tárhely szolgáltatására és annak biztonságának biztosítására.

Egy másik sebezhetőségi lehetőség lehet, ha olyan közismert weboldalmotort használunk, amellyel kapcsolatban már számos biztonsági rést feltártak és ezt használják ki a hackerek. Egy egyedi fejlesztés sem jelent teljeskörű biztonságot, viszont ez esetben a támadónak fel kell tárnia, hogy hol lehet biztonsági probléma a weboldallal, míg egy közismert weboldal motor esetén már előre kidolgozott módszerekkel próbálják feltörni a weboldalt. Ugyanakkor ezeket a weboldalmotorokat folyamatosan fejlesztik, így arra kell csak törekednünk, hogy mindig frissítsük, amikor valamilyen javítás jelenik meg a weboldalhoz. Gyakran ezek a frissítések automatikusan lefutnak, a weboldal üzemeltetőjének csak egyszerűen el kell indítania a frissítést.

A weboldalak egy másik közismert támadási felületei a különböző adatbeviteli mezők, ahol a látogatók megadhatják a belépési adataikat (felhasználónév és jelszó) vagy pedig kereséseket indíthatnak.

Azonban **nemcsak a hackerek okozhatnak problémát weboldalunk számára, hanem az elektronikus vírusok is**. Ezek a vírusok nemcsak a felhasználók számítógépeit támadhatják meg, hanem a weboldalakat is. Mindez úgy történhet, hogy ha a felhasználó elindítja a vírust (például email-en keresztül), akkor a vírus felmásolja magát a számítógépre. Ezt követően a vírus olyan adatokat keres, amelyek segítségével el tudja érni a weboldalunkat futtató szervert. A szervert megtámadva pedig már lehetősége van a weboldalunk megfertőzésére és szintén más weboldalak további támadására.

Jelen tananyag a Szegedi Tudományegyetemen készült az Európai Unió támogatásával. Projekt azonosító: EFOP-3.4.3-16-2016-00014

6.3. Mit tehetünk megoldásként?

Felmerül a kérdés, hogy mit tehet a vállalkozó annak érdekében, hogy a webáruháza biztonságos legyen a vásárlói számára. Az alábbiakban néhány egyszerű tanács kerül megfogalmazásra, amelyek nem helyettesítenek egy IT biztonsági szakembert, viszont ezek által kiküszöbölhetők a leggyakoribb IT biztonsági hibák:

1. Mindig frissítsük a weboldalmotort!
2. Frissítsük a szerveren található tűzfalat!
3. Frissítsük a vírusvédelmet biztosító szoftvert!
4. Ne mentsünk el böngészőben és/vagy tároljunk a számítógépen tárhely belépéshez szükséges adatokat!
5. Folyamatosan készítsünk biztonsági mentés a weboldalunkról!
6. A weboldalunkkal kapcsolatban állítsunk be korlátozást a belépéshez kapcsolódóan, például területi korlátozást vagy IP cím alapú korlátozást!

Jelen tananyag a Szegedi Tudományegyetemen készült az Európai Unió támogatásával. Projekt azonosító: EFOP-3.4.3-16-2016-00014