Követendő gyakorlat a kéretlen tömeglevelek elleni harcban

Richard Clayton,
Demon Internet.
1999. május 18.

Verziószám: 1.02

2000. március 7.
Dokumentum: ripe-206

Magyar nyelvű változatát az Internet Szolgáltatók Tanácsa elfogadta: 2004. október 18-án

---

Tartalom

Bevezetés

A kéretlen tömeglevél (Unsolicited Bulk Email, UBE, továbbiakban KTL) az Internet széles körben elterjedt problémája. Néha nevezik "szemétlevélnek" vagy "spamnek" is. A küldött mennyiség és a válogatás nélküli szétküldés miatt sok felhasználónak van tapasztalata elsőkézből KTL fogadásában, gyakran jelentős mennyiségben.

KTL küldése elfogadhatatlan, mert:

* az Internet működését gátolja.

  Több rendszer összeomlott már csupán a küldött levelek puszta tömegétől. A feladók gondoskodtak róla, hogy a kézbesítési hibajelzések kívülálló személyekhez érkezzenek, ezáltal jelentős problémákat okozva tevékenységükben. Mindezen súlyos elégtelenségek mellett, a KTL pusztán jelenlétével gyengíti a levelezőrendszereket, a szabályszerű forgalmat késleltetve illetve feltartva. Ezek a hatások messze az Interneten túl is jelentkeznek, minden olyan rendszerben, ami elektronikus leveleket továbbít.

* a fogadók számára felesleges forgalmat teremt.

  A legtöbb esetben a felhasználók fizetnek a kapcsolatukért, így olyasvalaminek a fogadását pénzelik, ami már eredetileg sem volt kívánatos.

* a szolgáltatóknak üzemeltetési többletköltséget okoz.

  A szolgáltatóknak nemcsak a saját, KTL-eket kapott ügyfeleitől származó panaszokkal kell foglalkozniuk, hanem mások által benyújtott jelentésekkel is, ami intézkedéseket igényel, amennyiben az ő ügyfelük küldte a szemétlevelet.

Továbbá:

* Üzleti formájában a szemétlevél általában bizonytalan származású, megkérdőjelezhető törvényességű és kétes termékeket népszerűsít.

* Nem létezik megfelelő rendszer a KTL szabályozására.

* Tevékenységük kihatásainak csökkentéséhez a szemétlevelet küldő személyek és cégek nem mutatnak hajlandóságot az Internet szolgáltatókkal történő hathatós együttműködésre.

* A szemétlevelet ritkán küldik azoknak, akik méltányolnák. A feladónak szinte semmibe sem kerül a szemétlevelek küldése. Ez kizár minden ösztönzést a terjesztés korlátozására. Valódi félelmeink egyike, hogy a szemétlevél-jelenség határtalanná nőhet és túltelítheti az egész Internetet valamint minden felhasználójának levelesládáját.

A KTL elküldés utáni megakadályozása igen erőforrásigényes és emiatt nem hatékony az internetszolgáltatók (Internet Service Provider, ISP, továbbiakban szolgáltató) számára, így a jelenlegi követendő gyakorlat (Best Current Practice, BCP, továbbiakban ajánlás) nem tárgyalja ennek módszereit. A KTL elleni harcban a szolgáltatók legkritikusabb közreműködése abból áll, hogy minimalizálják vagy teljesen megszüntessék ügyfeleik KTL küldését a szolgáltató rendszereiről. Az ajánlás célja, hogy ennek eléréséhez ismertesse a szolgáltatók jelenlegi kollektív véleményét a követendő gyakorlatról.

Amellett, hogy a szolgáltató saját érdeke a követendő gyakorlat alkalmazása, sok szolgáltató szeretné nyilvánosságra hozni, hogy mindent megtesznek a KTL elleni harcban. Ezért várható, hogy a szolgáltatók formálisan is szeretnék kijelenteni, hogy alkalmazzák a jelen követendő gyakorlatot. Ehhez segítségképpen a dokumentum szabványszövegezésű, a KÖTELES, KELL, LEHET és TILOS fogalmakat használva, ahogyan azt az RFC 2119 definiálja (összefoglalóhoz lásd D függelék).

A szolgáltatók KTL elleni hatékony küzdelméhez a követendő gyakorlat az alábbi.

1. A szolgáltató KÖTELES gondoskodni arról, hogy levelezőrendszere ne tegye lehetővé, hogy jogosulatlan harmadik személy a rendszer közvetítésével leveleket küldjön ki (relay).
2. A szolgáltató KÖTELES gondoskodni róla, hogy minden, saját hálózatában keletkezett levél visszakövethető legyen a forrásáig; valamint KÖTELES biztosítani a más hálózatokból érkező levelek közvetett forrásának megállapíthatóságát.
3. A szolgáltató KÖTELES biztosítani, hogy minden, saját hálózatában keletkezett levél hozzárendelhető legyen valamelyik ügyfélhez vagy rendszerhez.
4. A szolgáltató KÖTELES megtenni a megfelelő intézkedéseket az ügyfelei visszaéléseiről érkező jelentések kezelésére.
5. Ha a visszaélés bebizonyosodott, a szolgáltató KÖTELES megakadályozni az ügyfél által további KTL küldését. A szolgáltatások biztosításához alkalmazott jogi alap KÖTELES lehetővé tenni az ilyen irányú intézkedéseket.
6. A szolgáltató KÖTELES nyilvánosságra hozni a KTL-t küldő ügyfelekkel szemben alkalmazott intézkedéseit.
7. A szolgáltató KÖTELES ügyfeleivel megismertetni a KTL jellegét és KÖTELES ügyfelei tudomására hozni, hogy KTL küldése elfogadhatatlan magatartásnak minősül.

Ezen hét pont kifejtve alább olvasható.

A kiterjesztett magyarázatokkal együtt felsorolunk néhány feltételt, amelyeket a szolgáltató KÖTELES ügyfeleivel szemben alkalmazni. Szükséges lesz biztosítani, hogy a szolgáltató és az ügyfél között létrejövő szerződés alapján a szolgáltatónak jogában álljon ilyen feltételeket támasztani, valamint elfogadhatatlan magatartás esetén az ügyféltől a szolgáltatásokat megvonni.

A szolgálatók közötti fair verseny biztosításához, azaz hogy ne lehessen marketing előnyhöz jutni a kötelezettségek kijelentésének elhagyásával, a szolgáltató HASZNÁLHATJA a C függelékben lefektetett szabvány cikkelyeket és KÖTELES használni ezeket vagy más cikkelyeket, amelyek legalább ennyire hatásosak. A szolgáltató ELHELYEZHETI ezeket a cikkelyeket egy általánosabb elfogadható felhasználási szabályzatban (Acceptable Use Policy, AUP) amely további visszaélési helyzeteket tárgyal.

Ezen dokumentumban foglalt rendelkezéseknek minden ügyfélre érvényesnek kell lenniük. Ugyanakkor néhány ügyfélnek lesznek saját ügyfelei. A szolgáltató úgy tehet eleget a követendő gyakorlatnak, hogy biztosítja, hogy az ilyen ügyfelek alkalmazzák ugyanezeket az elveket és a követendő gyakorlat eljárásait saját ügyfeleikkel szemben is.

Az A függelék tartalmazza a fogalommagyarázatokat, de különösképpen ebben a dokumentumban a "szolgáltató" fogalma nemcsak a legfelső szintű internetkapcsolatok szolgáltatóit takarja, hanem az ilyen szolgáltatók minden ügyfelét is, amelyek "rekurzívan" alkalmazzák ezeket az elveket a saját ügyfeleikkel szemben. Hasonlóképp, az "ügyfél" fogalma nemcsak a formális szerződésbeli kapcsolatokra vonatkozik, hanem minden olyan esetre, mikor valaki a szolgáltatások "felhasználója".

1. Nyílt levéltovábbítás tiltása

Leírás

Az SMTP protokollt használó levelezőrendszerek hagyományosan bárkitől elfogadtak levelet és kézbesítették a címzettnek, vagy továbbították a tényleges címzett felé. Ez a nyílt közvetítés a levelek továbbításában nagyon robusztussá tette az elektronikus levelezést, hiszen egy gép kisebb konfigurációs hibáin úrrá lehetett egy másik gép, amelyik pontosabb információkkal rendelkezett a levél továbbításának lehetőségeiről. Az egész Internetet átható együttműködés szellemében a gépek tulajdonosai hajlamosak voltak nem naplózni az ilyen továbbításokat, a megakadályozásáról nem is szólva.

A Domain Name System (DNS) és a sokkal jobb kapcsolatok megjelenésével az ilyen fajta közvetítő funkcióra való igény régen megszűnt. Ugyanakkor a funkcionalitás megmaradt a levélkezelő programokban.

Sajnálatos módon az utóbbi időben gátlástalanul visszaélnek ezzel a nyílt levéltovábbítási (open mail relay) funkcióval, hosszú címzettlistákat tartalmazó leveleket küldve. Ez mások rendszerét több példány levél generálására készteti, más és más címzettel. A leveleket így megsokszorozva, a KTL küldője más rendszerek erőforrásait használja a KTL sokszorosításához. Továbbá, a küldő számára lehetőség adódik egy gyengén konfigurált rendszeren a KTL igazi származási helyének eltitkolására, vagy legalábbis a kevésbé képzettek félrevezetésére a származási hely megállapításában.

Mivel már rég nincsen rá szükség és visszaélésre ad lehetőséget, napjainkban igen helytelen a levéltovábbító rendszerek olyan beállítása, amely lehetővé teszi jogosulatlan személyek kezdeményezésére levelek továbbítását, közvetítését.

Sok, jelenleg is működő kezdeményezés található az Interneten a még mindig közvetítést végző rendszerek azonosítására. Tipikusan az ilyen rendszerek tiltólistákra kerülnek, amelyek a levelek terjedését befolyásolják. Még ha valaki nyílt levéltovábbítót szeretne is üzemeltetni, közeleg az idő, amikor csak nagyon kevesen lesznek hajlandóak az ilyen rendszerekkel együttműködni.

Általánosan elfogadott, hogy a szolgáltatók ún. "smarthostot" üzemeltetnek, amely ügyfeleik számára levéltovábbítást biztosít, különösképp a telefonos behívókapcsolattal és helyi hálózattal rendelkezőknek. Ez szükségtelenné teszi, hogy ezen ügyfelek gépei teljes funkcionalitású kézbesítőrendszereket futtassanak. Ez a módszer egyfajta levéltovábbítás, de természetesen teljesen elfogadott gyakorlat, feltéve, hogy a smarthost visszautasítja a jogosulatlan gépek által küldött levelek továbbítását.

Követelmények

A szolgáltatók KÖTELESEK levelezőrendszerüket úgy beállítani, hogy jogosulatlanok leveleinek közvetítését ne engedélyezzék. A szolgáltatóknak el KELL fogadni leveleket a saját ügyfeleiktől, valamint TEHETNEK privát intézkedéseket más rendszerek leveleinek továbbítására.

A szolgáltatók KÖTELESEK megakadályozni, hogy ügyfeleik nyílt levéltovábbítást végezzenek. Ha a szolgáltató ilyen rendszer üzemeléséről értesül, akkor KÖTELES lépéseket tenni a rendszer Internetről való eltávolítása érdekében, amíg a tevékenység korrigálásra nem kerül.

A szolgáltatónak AJÁNLOTT időnként ellenőrizniük, hogy ügyfeleik, különösen az állandó kapcsolattal rendelkezők, nem üzemeltetnek-e nyílt levéltovábbítókat. Ahol ez biztonsági megfontolásokból nem lehetséges, vagy ahol a kapcsolat megszakított, a szolgáltatónak AJÁNLATOS biztosítania, hogy az ügyfelek képesek legyenek ezt az ellenőrzést saját részükre elvégezni. A szolgáltató eszközöket

BIZTOSÍTHAT, például a weben, hogy az ügyfelek elvégezhessék saját ellenőrzésüket.

A B függelék mutatókat tartalmaz technikai információkra, hogy hogyan ellenőrizhető a nyílt levéltovábbítás letiltottsága.

A C függelék szerződés-példacikkelyeket tartalmaz egyes követelmények megfogalmazására, alkalmazására.

2. A rendszeren átmenő levelek nyomonkövethetősége

Leírás

Ahhoz, hogy a levelek nyomonkövethetők legyenek a forrásukig, minden rendszernek meg kell felelnie az email szabványoknak és egy "Received" fejlécsort kell hozzáadniuk a levélhez, amikor az áthalad rajtuk. Ez szolgál a fejlécet hozzáadó gép és a levelet ennek továbbító gép azonosítására. Elméletileg a legrégebbi ilyen sor a levél forrását jelöli. Gyakorlatilag azonban ez néha hamis és az igazi küldő visszakereséséhez egyesével meg kell vizsgálni a Received fejlécsorokat, amíg például időbeli szakadást nem találunk (néha még ezzel a módszerrel sem lehet megállapítani a hamisítást).

A levelek küldői néha megpróbálják a levél eredetét elfedni a forrásgép nevének meghamisításával a "HELO" protokollparancsban. Ez a fajta hamisítás könnyen észlelhető, ha biztosítjuk, hogy a Received fejlécsor nem csak a küldő rendszer nevét, hanem IP címét is tartalmazza, mivel ez utóbbit nem lehet elrejteni.

Követelmények

A szolgáltatók KÖTELESEK gondoskodni a szabványnak megfelelő "Received" fejlécsor hozzáadásáról, amint a levelek áthaladnak rendszereiken.

A szolgáltatók KÖTELESEK gondoskodni a nekik levelet küldő gép azonosságának rögzítéséről. A HELO bejelentkezésben használt nevet TILOS érvényesnek tekinteni és az IP címet fel KELL jegyezni.

3. A levél feladójának azonosítása

Leírás

A 2-es pont gondoskodik róla, hogy a levelek visszakövethetők legyenek a küldő IP címéig.

Telefonos behívó kapcsolatoknál szokás "dinamikus IP-t" használni, azaz ugyanazt a címet újra kiadni más ügyfeleknek. Az ISDN kapcsolatok esetleg csak pár másodpercig tartanak, tehát elméletileg egy IP címet szinte azonnal újra használhat egy teljesen más személy.

Azonban az IP cím és a kapcsolat időpontja egyértelműen azonosítja a levél küldőjét. Tehát szükség van a pontos idő rögzítésére minden Received sorban. Ennek az időpontnak és a küldő szolgáltató egyéb naplóinak tartalma a küldő egyértelmű azonosítására szolgál.

A fenti leírás csak felületesen érintett egy nagyon összetett témát. A LINX Jelenlegi Követendő Gyakorlat dokumentum a "Nyomonkövethetőség" fejezetben (lásd B függelék) további információt és tanácsokat tartalmaz.

Követelmények

A szolgáltatók KÖTELESEK gondoskodni a levelezőrendszerük órájának, időpecsétjének pontosságáról.

A dinamikus IP címek rövid időn belül újra felhasználhatók. A szolgáltatóknak ezért NTP-alapú időbélyegeket, vagy ezzel egyenértékű protokollt használniuk, ami az időt rendszeresen referenciaértékekkel hasonlítja össze és másodpercnél jobb pontosságot nyújt.

A szolgáltatók KÖTELESEK más naplókat is ésszerű időtartamig megőrizni, hogy képesek legyenek egy adott dinamikus IP címnek, amelyet egy adott időben használtak, azt az ügyfelet megfeleltetni, aki egy esetleges visszaélésért felelősségre vonható.

Kivétel

A (2) és (3) pontok alól kivételt képez az az eset, mikor egy rendszert úgy üzemeltetnek, hogy szándékosan fedje el az email feladóját; ezeket gyakran "névtelen kiszolgálóknak" (anon szerver) nevezik. A névtelen kiszolgálók az anonimitás megőrzésére használhatók például bántalmazottakat támogató csoporttól való segélykérésre vagy politikai nézetek kifejezésére olyan országban, amely bünteti a véleménykülönbséget.

A szolgáltatók és ügyfeleik ÜZEMELTETHETNEK névtelen kiszolgálókat abban az esetben, ha kifejezetten ez a funkciója a szolgáltatásnak. Ugyanakkor TILOS az általános szolgáltatás által névtelenséget biztosítani úgy, hogy az nem teljesíti ezen dokumentum kívánalmait.

Ugyanakkor egy névtelen kiszolgálónak NEM KELLENE képesnek lennie levelek "többszörözésére" címlisták kifejtésével, sőt korlátozó mechanizmusokkal KELL rendelkeznie annak biztosítására, hogy a kiszolgálón átmenő levélforgalom ne lehessen szokatlanul nagy a rendszer tulajdonosának tudta nélkül.

4. Visszaélés-jelentések kezelése

Leírás

A szolgáltatóktól elvárjuk, hogy fogadják és dolgozzák fel az ügyfeleik visszaéléséről szóló jelentéseket.

Ha egy ügyfél KTL-t küld, a panaszok várhatóan a szolgáltatóhoz érkeznek. Ezeket a panaszokat, megegyezés szerint, általában a "postmaster"-nek címzik. Az utóbbi időben kívánatos lett, hogy az ilyen leveleket az erre a célra szolgáló "abuse" címre küldjék. Ez a gyakorlat teljességében először az RFC2142-ben lett dokumentálva.

Mikor panasz érkezik, célszerű azonnal nyugtázni, esetleg csupán egy szabvány üzenettel, ami a helyi irányvonalakat és módszereket taglalja.

Kívánatos egy ún. "ticketing" rendszert használni, ami lehetővé teszi az incidensek nyilvántartását, feldolgozását. Ez segít a jelentések összekapcsolásában és az eredeti panaszostól származó további levélváltások egybevetésénél is.

Szintén kívánatos a panaszosoknak válaszolni és elmagyarázni, hogy milyen döntés született. Néha, különösen mikor nagyon sok jelentés érkezik egyszerre, ez nem túl praktikus. A fentebb vázolt szabvány válaszlevél tartalmazhat utalásokat későbbi lehetséges válaszra, illetve webcímeket ahol a szolgáltató által tett lépések kerülnek feljegyzésre (lásd (6) lejjebb).

Követelmények

A szolgáltatók KÖTELESEK jelentéseket fogadni az abuse@domain formájú címen, ahol a domain az ügyfelek által használt domain, vagy abban az esetben, ahol az ügyfél domainje egy generikus domain aldomainje, az abuse címnek a generikus domainben kell élnie.

tehát ahol az ügyfelek címe ilyen alakú:

ugyfel@isp.com

a támogatott abuse-cím:

abuse@isp.com

ahol az ügyfelek címe ilyen alakú:

email@ugyfel.isp.com

a támogatott abuse-cím:

abuse@isp.com

Ha kívánja, a szolgáltató FOGADHAT jelentéseket más abuse címeken is (pl. abuse@isp.net), de TILOS elvárnia a jelentés újraküldését másik címre, mielőtt reagálna rá.

A szolgáltatónak dokumentálnia KELL ezen címek meglétét a cég weboldalain, valamint közölnie KELL a panaszok feldolgozásához szükséges, általa megkívánt információkat, amit a bejelentésnek tartalmaznia kell.

A szolgáltató KÖTELES nyugtázni a visszaélés-jelentések érkezését (amennyiben ez utóbbit nem egy automata rendszer küldte, mely felhívja a figyelmet a válaszküldés fölöslegességére) és kezelő rendszert KELL használnia a jelentések nyomkövetésére.

5. Reagálás visszaélés-jelentésekre

Leírás

Nincs elfogadható indok kéretlen tömeglevelek küldésére.

Azokon kívül, akik arra hivatkoznak, hogy nincsenek tisztában a KTL elfogadhatatlan jellegével (lásd a Követelmények szekciót lejjebb), a legnépszerűbb magyarázat az, hogy a küldött levelek nem voltak kéretlenek.

Ahhoz, hogy elfogadja ezt a magyarázatot, a szolgáltatónak meg kell vizsgálnia, hogy a küldő hogyan jutott hozzá a címekhez. Az adatvédelmi szabályozások általában megkövetelik, hogy az információt jogszerűen kezeljék. Jelen esetben a szolgáltatónak kell kielégítő válaszokat találni a következő kérdésekre:

- Tudatában voltak-e az érintettek, hogy címeiket összegyűjtik?
- A küldött levél egyértelműen kapcsolható-e a címgyűjteményhez?
- Volt-e lehetőségük a címzetteknek a levelek elutasítására?
- A címzettek visszavonhatják-e korábbi belegyezésüket?

A kérdések lényege, hogy egy Usenet cikk küldése vagy szimplán egy weboldal megtekintése NEM számít felhatalmazásnak tömeglevelek küldésére. Hasonlóképpen, harmadik személytől szerzett címlisták sem jelentik azt, hogy az ügyfél jogszerűen küld levelet azokra a címekre.

Világos, hogy ha valaki explicit feliratkozott egy levelezési listára, akkor az onnan érkező levél jogszerű. Ugyanakkor a valós világban van néhány hosszú ideig szunnyadó levelezési lista és a rájuk feliratkozottak emlékezőtehetsége korlátozott. Amikor ilyen listáról érkezik levél, előfordulhat, hogy kéretlen levélként jelentik a levelezési lista szolgáltatójánál. Mivel ugyanaz a szoftver használható levelezési lista céljára illetve KTL küldésére is, a szolgáltatónak a fentiek alapján kell különbséget tenni a két eset között.

Levelezőlista-tulajdonosok demonstrálhatják felelős viselkedésüket pontos naplók vezetésével. Ideális esetben fel tudják mutatni a feliratkozást igénylő levél másolatát, illetve a feliratkozáskor válaszlevél nyugtáztatással meggyőződhetnek róla, hogy nem egy harmadik személy kezdeményezte rosszindulatúan a feliratkozást. Természetesen alapvető, hogy a nem kívánt levél címzettje leiratkozhasson a listáról. A modern levelezőlista-szoftvercsomagok automatizálják ezeket a módszereket.

Mint a dokumentum elején is említettük, a szolgáltatóknak lehetnek olyan nagy ügyfelei, akik saját maguk alkalmazhatják jelen ajánlást és menedzselhetik saját ügyfeleiket vagy felhasználóikat. Ezekben az esetekben a szolgáltató támaszkodhat ügyfelére a KTL küldőjének kezelésében és nem kell alkalmaznia az alább tárgyalt szankciókat, mint például a nagy ügyfelek lekapcsolása az Internetről. Ugyanakkor a szolgáltató továbbra is felelős a szélesebb közösség felé, amely elvárja, hogy a szolgáltató elfogadható mértékben biztosítsa, hogy ügyfele tényleg megteszi a szükséges lépéseket a szolgáltató helyett.

Követelmények

A szolgáltató KÖTELES reagálni a bizonyított KTL küldeményekre és KÖTELES biztosítani, hogy az ügyfeleivel kötött szerződés a hatékony beavatkozásra lehetőséget adjon.

A szolgáltató KÖTELES gondoskodni róla, hogy az állítólagos visszaélést elkövető NEM értesül a jelentést tevők személyazonosságáról, kivéve azok explicit engedélyével.

A szolgáltató azonnal ZÁROLHATJA az ügyfél azonosítóját.

Ugyanakkor, mivel a tudatlanság, hogy mi elfogadható és mi nem, továbbra is népszerű magyarázat a visszaélésekre, előfordulhat, hogy nem állapítható meg pontosan az eset jellege. A szolgáltató ALKALMAZHATJA az ún. "két csapás" irányelvet, azaz továbbra is engedélyezheti az azonosító használatát a következő szabálysértésig.

Amennyiben a "két csapás" irányelvet alkalmazza, a szolgáltatónak külön lépéseket KELL tennie az első szabálysértésen kapott ügyfelek okítására az elfogadható viselkedésről illetve ELVÁRHATJA az ügyféltől, hogy az újbóli internethasználat engedélyezése előtt kötelezettségvállalást írjon alá, miszerint nem szegi meg többször a szabályokat.

Amennyiben második szabálysértés történik az elsőtől számított hat hónapon belül, a szolgáltató KÖTELES zárolnia az ügyfél azonosítóját és minden hozzá tartozó szolgáltatást. A küldő érintett email címének megszűntetése fontos szankció a KTL elleni harcban.

Sok ember nem veszi a fáradtságot a visszaélések jelentésére, mert úgy gondolja, hogy nem lesz eredménye. Emiatt a szolgáltató nem várhat nagyszámú, egymást megerősítő jelentéseket. Ebből kifolyólag már két, azonos levelet megjelölő jelentést KÖTELES tömeglevél küldésének bizonyítékaként kezelni.

Amennyiben a szolgáltató csak egyetlen jelentést kap egy visszaélésről, DÖNTHET arról, hogy azt nem elegendő bizonyíték miatt nem fogadja el. Ugyanakkor

értesítenie KELL az ügyfelét a jelentett visszaélésről és meg KELL ragadnia a lehetőséget, hogy emlékeztesse a kéretlen tömeglevél-küldés elfogadhatatlan voltára és a vele járó szankciókra.

A szolgáltató KÖTELES mérlegelni az összejátszás és hamisítás lehetőségét, valamint azt, hogy a jelentés esetleg csak utánzat. KÖTELES lehetőséget adni ügyfelének ártatlansága igazolására és KÖTELES ésszerűen eljárni a tényleges történések megállapításában.

Előfordulhat, hogy az ügyfél továbbra is állítja, a levelet jogszerűen küldte. A szolgáltatónak TILOS ezt elfogadnia, kivéve ha az ügyfél jogszerűen jutott a címhez és törvényesen kezelte azt.

Amennyiben a levelet levelezőlista-szoftveren keresztül küldték, a szolgáltató KÖTELES fontolóra venni, hogy a levél jogszerű volt, de erről a tényről a címzettek megfeledkeztek. Mindamellett a szolgáltatónak bátorítania KELL a listák tulajdonosait a feliratkozó levelek naplózására, hogy azok érvényessége megállapítható legyen. A szolgáltató KÖTELES gondoskodni róla, hogy az emberek egyszerűen leiratkozhassanak az ügyfelei által üzemeltetett levelezési listákról.

Ha a KTL küldője nem közvetlenül a szolgáltató ügyfele, a szolgáltató DELEGÁLHATJA jelen ajánlás betartatásának felelősségét az ügyfélre, amennyiben a szolgáltató megfelelő lépéseket tesz ennek érdekében.

6. Tájékoztatás az intézkedésekről

Leírás

Sok előnye van a KTL-t küldő ügyfelekkel szemben tett lépések publikálásának.

Amennyiben egy jelentés időben érkezik, megelőzheti a KTL más címzettjeitől érkező jelentéseket. Ez csökkenti a szolgáltató munkaterhelését.

Egy szolgáltató, amely beszámol az általa megtett lépésekről, növeli presztízsét a közösségen belül, mivel az emberek kedvezően tekintenek az olyan szolgáltatókra, amelyek keményen fellépnek a KTL küldőivel szemben. A szolgáltató pedig demonstrálja a potenciális visszaélőknek, hogy igenis valós kockázata van a lelepleződésnek és a szankcionálásnak.

Ugyanakkor alapvető, hogy az információközlés pontos és lényegretörő legyen, különben felmerül a rágalmazás veszélye.

Szükséges továbbá az adatvédelmi előírásoknak megfelelni. Ez nem feltétlenül igaz vállalatokra -- így teljes nevük és címük publikálható; de egyének esetén majdnem biztosan szükség van a pontos azonosítás elkerülésére, hacsak nem történtek szerződéses lépések ezen információk nyilvánosságra hozatalára visszaélés esetén.

Az ehhez hasonló beszámolók nem okozhatnak problémát: "<dátum>-on zároltuk a <hostname@isp.com> című azonosítót kéretlen tömeglevelek küldése miatt. Ezen azonosító által elkövetett visszaélések további bejelentése szükségtelen."

A nyilvános beszámoló mellett a szolgáltató szükségesnek tarthatja a saját szervezetén belüli tájékoztatást. Helytelen gyakorlat zárolt azonosítókat újra kiadni, vagy ugyanazon egyénnek név-, cím-, esetleg hitelkártya-egyezés alapján azonnal új azonosítót adni.

Követelmények

A szolgáltatók nyilvánosságra HOZHATJÁK a KTL ellen tett lépéseiket.

Amennyiben nyilvánosságra hozatal történik, a szolgáltatók KÖTELESEK a rágalmazást vagy az adatvédelmi törvény megsértését kerülni.

A szolgáltatóknak áttekintő statisztikákat KELL közölniük még akkor is, ha egyedi beszámolókat nem készítenek.

A szolgáltatóknak gondoskodniuk KELL róla, hogy a KTL küldéséért zárolt azonosítójú egyéneknek ne adjanak azonnal új azonosítót, hiszen nyilvánvalóan fennáll a további visszaélés veszélye.

7. Oktatás

Leírás

A szolgáltatóknak lépéseket kell tenniük ügyfeleik oktatására az elfogadható levelezési viselkedésről. Elfogadott tény, hogy a szolgáltatók nehézségekbe ütköznek ezen a téren, mert értékesítési osztályuk túlhangsúlyozhatja az Internet előnyeit és jelentéktelennek tüntetheti fel a hátrányos következményeket.

Sok visszaélés-jelentés nem tartalmaz alapvető információkat a szükséges lépések megtételéhez. A ügyfelek elfelejtik például a levél fejléc összes információját elküldeni, ami szükséges a küldő megfelelő azonosításához. Továbbá az ügyfelek néha szabadjára engedik indulataikat és ezzel halmozzák el a visszaélésekkel foglalkozó munkaerőt.

Mindenki felelőssége megpróbálni a jelenlegi helyzeten javítani, hogy kevesebb elégtelen vagy megkérdőjelezhető jelentés szülessen, az ilyen jelentésekkel foglalkozók kevesebb időt vesztegessenek, így minden érintett kevesebb csalódottságot tapasztal.

Követelmények

A szolgáltatók KÖTELESEK gondoskodni az ügyfelek részére hozzáférhető dokumentációról, ami elmagyarázza a KTL jellegét, küldésének elfogadhatatlanságát.

A szolgáltatók KÖTELESEK az ügyfeleket informálni arról, hogy mit kell egy visszaélés-jelentésnek tartalmaznia és hogyan kell ezeket megírni.

A függelék: Szójegyzék

AUP: Acceptable Use Policy (Elfogadható Felhasználási Szabályzat)
A szolgáltató és az ügyfél közötti szerződés kiegészítése, ami felsorolja, hogy az ügyfél mit és (főképpen) mit nem tehet amíg a szolgáltató erőforrásait használja.

BCP: Best Current Practice (Jelenlegi Követendő Gyakorlat)
Az iparág ismert jelenlegi követendő gyakorlat leírása.

DNS: Domain Name System
Nevek és IP címek közötti fordítást biztosító elosztott rendszer. Leírása az RFC1035-ben található.

HELO: Hello
Az SMTP email protokoll egyik parancsa, a távoli gép nevének bejelentésére szolgál.

IP: Internet Protocol
Az Interneten gépek közötti csomagcserére használt alapprotokoll. További protokollok épülnek rá a felhasználóknak nyújtott szolgáltatásokhoz. Leírása az RFC971-ben és RFC1122-ben található.

ISP: Internet Service Provider (szolgáltató)
A dokumentumban ez a fogalom az Internet kapcsolatot biztosító cégek és szervezetek általános leírására szolgál, valamint a szolgáltató olyan ügyfeleire, akik maguk is elfogadták és alkalmazzák ezt az ajánlást a saját ügyfeleikre a szolgáltató helyett.

KTL: Kéretlen TömegLevél
Explicit kérés nélkül nagy mennyiségben küldött levél. Nevezik néha "szemétlevélnek" vagy "spamnek" is. Jelenleg általában bizonytalan tulajdonú üzleti vállalkozások hirdetési anyagát tartalmazza. Lásd még UCE.

LINX: London Internet Exchange
A LINX egy teljesen semleges, szolgáltatók közötti nonprofit társulás, ami egy fő Internet csomópontot üzemeltet Angliában. Alapvetően az Internet-forgalom hatékony továbbítását mozdítja elő, ugyanakkor érdekelt a tagjai számára közérdekű tevékenységekben. Egyik ilyen tevékenysége a "tartalomszabályozással" kapcsolatban tartalmazta ennek a dokumentumnak az elkészítését. Lásd: http://www.linx.net/

NTP: Network Time Protocol
A pontos idő megállapítására szolgáló protokoll, leírása az RFC1119-ben és az RFC1305-ben található.

RFC: Request for Comments
Az Internetről (eredetileg az ARPANET-ről) szóló, 1969-ben indított jegyzetsorozat. A jegyzetek több szempontból tárgyalják a számítástechnika és számítógépes kommunikáció témáját a hálózati protokollokra, módszerekre, programokra és fogalmakra fókuszálva, de tartalmazza megbeszélések jegyzeteit, véleményeket és néha humort is. Az Internet szabványai RFC dokumentumokban vannak lefektetve. Lásd: http://www.rfc-editor.org/

SMTP: Simple Mail Transfer Protocol
Email továbbító protokoll. Leírása az RFC821-ben és RFC1123-ban található.

UBE: Unsolicited Bulk Email
 lásd KTL

UCE: Unsolicited Commercial Email (Kéretlen Üzleti Levél)
 Némely értekezések különbséget tesznek az üzleti jellegű és nem üzleti
 jellegű kéretlen levelek között. Jelen dokumentum ugyanúgy
 elfogadhatatlannak tartja, mint önmagában a KTL-t, elkerülve így a
 tartalom üzleti vagy nem üzleti besorolásának igényét.

B függelék: Referenciák és olvasnivalók

[Megjegyzés: a dokumentum kiadója nem vállal felelősséget a kívülállóharmadik személy által készített oldalak tartalmáért, nem szükségképpenhagyja jóvá a tartalmukat és természetesen ezek a linkek nem biztos, hogymindig szabatosak lesznek a jövőben.]

Sok oldal található az Internetet ami a kéretlen leveleket tárgyalja általánosságban. Néhány érdekesebb közülük:

 * CIAC I-005c: Email spam ellenintézkedések

 http://ciac.llnl.gov/ciac/bulletins/i-005c.shtml

 * "Harcolj a spam ellen az Interneten"

 http://spam.abuse.net/

 * Kéretlen Üzleti Levelek Elleni Egyesülés

 http://www.cauce.org/

 * Kéretlen Üzleti Levelek Elleni Európai Egyesülés

 http://www.euro.cauce.org/

Minden levelezőszoftver oldalán majdnem biztosan tárgyalják a jogosulatlan, nyílt levéltovábbítás megelőzését. Például:

 * Sendmail

 http://www.sendmail.org/antispam.html

 * Exim

 http://www.exim.org/howto/relay.html

 * Qmail

 http://qmail-docs.surfdirect.com.au/docs/qmail-antirelay.html

 * Exchange Server

 http://support.microsoft.com/support/kb/articles/q196/6/26.asp

A levelezőszerverekről szóló információmutatók széles körű gyűjteményéhez lásd a MAPS Transport Security Kezdeményezést:

 http://maps.vix.com/tsi/

Léteznek általános termékek amelyek több rendszerrel együtt használhatók a

levéltovábbítás ellenőrzésére. Egy üzleti példa:

http://www.mailshield.com/

Saját rendszerének jogosulatlan levéltovábbítási lehetőségének ellenőrzéséhez:

http://maps.vix.com/tsi/ar-test.html

LINX Jelenlegi Követendő Gyakorlat "Nyomonkövethetőség"

http://www.linx.net/noncore/bcp/traceability-bcp.html

C függelék: Példacikkelyek

A következőkben cikkelyek olvashatók, amelyeket a szolgáltatók felhasználhatnak Általános Szerződési Feltételeikben a KTL küldői elleni szankciók kikényszerítésének támogatásához, ahogyan a jelenlegi ajánlás tartalmazza. Ezekben a cikkelymodellekben a szolgáltatóra "Szolgáltató"-ként, az ügyfélre pedig "Ügyfél"-ként hivatkozunk. A szolgáltatók lecserélhetik ezeket a saját dokumentumaikban használt
fogalmakra.

Általános cikkely az intézkedés lehetőségéhez

A Szolgáltató időről időre az általa nyújtott szolgáltatásokhoz Elfogadható Felhasználási Szabályzatot (AUP) tesz közzé. Az Ügyfél a szolgáltatás igénybevételének feltételeként köteles alávetni magát az AUP-ban foglaltaknak. Amennyiben ennek nem tesz eleget, a Szolgáltató fenntartja kizárólagos döntési jogát az azonosító megszüntetéséről, előzetes értesítés és kártérítés nélkül, valamint esetleges további követelések támasztásához vagy a kérdéses szolgáltatáshoz való hozzáférés megtagadásához.

Általános cikkely a pásztázás engedélyezéséhez

A Szolgáltató saját belátása szerint futtathat kézi vagy automatikus rendszereket annak feltárására, hogy az Ügyfél eleget tesz-e az AUP-nek (pl. nyílt levéltovábbítók pásztázása). A Szolgáltató úgy tekinti, hogy az Ügyfél engedélyezi hálózatának vagy gépének ilyetén ellenőrzését.

AUP cikkely a kéretlen tömeglevelek küldésének elutasításához

Az Ügyfél nem használhatja azonosítóját kéretlen tömeglevelek küldésére. Az Ügyfélnek explicit engedéllyel kell rendelkeznie minden címzettől nagyobb mennyiségű levél küldése előtt.

Az Ügyfél nem tekintheti engedélyezésnek a passzív tevékenységeket, mint például egy Usenet cikk küldése vagy egy weboldal megtekintése.

Azokban az esetekben, mikor az Ügyfél explicit engedéllyel rendelkezik, akár egy weboldalon vagy más kapcsolaton keresztül, naplót kell vezetnie ezekről az engedélyekről és köteles beszüntetni további levelek küldését, ha erre felkérik.

AUP cikkely jogosulatlan levéltovábbítás tiltásához

Az Ügyfél köteles gondoskodni róla, hogy nem küld tovább másoktól származó kéretlen tömegleveleket. Ez vonatkozik mind az Ügyfél rendszeréből, mind az Ügyfél rendszerén esetleg áthaladó, másoktól származó levelekre.

A tiltás nem csak a nyílt levéltovábbító működésére vonatkozik, hanem minden olyan gépre amely jogosulatlan vagy ismeretlen feladóktól elfogad levelet és

továbbítja az Ügyfél gépén vagy hálózatán kívüli címzettnek. Amennyiben az Ügyfél gépe jogosultan továbbít leveleket, úgy köteles feljegyezni a rendszeren való áthaladás tényét a megfelelő "Received" sorban.

A levéltovábbítás tiltása és a "Received" sor elhelyezésének kötelessége alól kivételt képez az Ügyfél által futtatott névtelen levéltovábbító szolgáltatás, feltéve, hogy az Ügyfél folyamatosan felügyeli oly módon, hogy észlelhető legyen a jogosulatlan vagy túlzó felhasználás.

D függelék: Követelmények kulcsszavai

Az alábbiak egy rövid összefoglalása az RFC2219 "RFC-kben használatos kulcsszavak követelményszintek jelzésére" dokumentumnak. További iránymutatóként ajánljuk az Olvasónak a teljes dokumentum megtekintését.

KÖTELES

Ez a szó abszolút követelményt jelent.

TILOS

Ez a szó abszolút tiltást jelent.

KELL

Ez a szó azt jelenti, hogy előfordulhatnak bizonyos esetek, mikor a kérdéses pontot figyelmen kívül hagyják, de mielőtt ezt megtennék, az összes következményt pontosan ismerni és mérlegelni kell.

NEM KELLENE

Ez a kifejezés azt jelenti, hogy előfordulhatnak bizonyos esetek, mikor a kérdéses viselkedés elfogadható vagy éppen még hasznos is, de az így jelölt viselkedés implementálása előtt az összes következményt pontosan ismerni és mérlegelni kell.

LEHET, -HAT/-HET

Ez szó azt jelenti, hogy a kérdéses pont teljesen opcionális.

A dokumentum eredeti, LINX-féle verziója bizonyos Anglia-specifikus hivatkozásokat tartalmaz és a http://www.linx.net/noncore/bcp/ube-bcp.html címen található.
