National Datacenter

ХАЛДЛАГАД ХАРИУ ҮЙЛДЭЛ ҮЗҮҮЛЭХ БАГ

2017 он

“PGP” түлхүүрийн тухай

1. “PGP” түлхүүр гэж юу вэ?

“Pretty Good Privacy” (PGP) нь цахим орчинд өгөгдөл дамжуулалтыг баталгаажуулж шалгахад ашиглах боломж бүхий шифрлэлтийн програм юм. “PGP” нь цахим орчинд хувь хүнийг мөн гэдгийг илэрхийлэх цахим гарын үсэг гэж ойлгож болно.

PGP нь аюулгүй байдлын хүртээмжтэй, нууцлагдсан, бүрэн бүтэн байдлыг хангах боломжтой бөгөөд бөгөөд текст, файл зэргийг баталгаажуулах, шифрлэх, буцаан задлахад ашигладаг. Мөн цахим шуудангийн аюулгүй байдлыг нэмэгдүүлэхэд өргөн хэрэглэдэг.

PGP ассиметрик буюу хос түлхүүр үүсгэн ашиглана. “RSA” алгоритм ашиглан нууцлал хамгаалалтыг хийдэг ба 1024, 2048, 4096 битийн урттай түлхүүр үүсгэх боломжтой.

Нийтийн түлхүүр /public key/ – бусдад ил байх бөгөөд өгөгдөл дамжуулалт хийхэд ашиглана.

Хувийн түлхүүр /private key/ – бусдаас далд байх шаардлагатай бөгөөд нууц үгийг зөвхөн өөрөө мэдэх үсэг тоо тэмдэгт орсон 8 дээш урттай мартаж болохгүй нууц үгээр хамгаалсан байх шаардлагатай.

2. “PGP” түлхүүрийг яагаад ашиглах шаардлагатай вэ?

Мэдээллийн технологийн хөгжил нь өнөө цагт нийгэм эдийн засгийг хурдасгагч гол хүчин зүйлүүдийн нэг болж, өдөр тутмын хэрэглээ өссөн нэмэгдэхийн хэрээр цахим мэдээллийн аюулгүй байдлын асуудлууд ч мөн тулгарч байна. Интернет орчинд өгөгдөл солилцоход мэдээлэл алдагдсан эсэх, дундаас нь мэдээллийн агуулгыг өөрчилсөн эсэх зэрэг нотлох, баталгаажуулах, баттай эх сурвалжийг тогтоох шаардлага үүссэн бий болж байдаг. Энэ баталгаажуулалтыг хийж мэдээллийн бүрэн бүтэн, хүртээмжтэй, нууцлагдсан байдлыг хангаж байгаа хэрэгсэл, програм хангамж бол “PGP” юм. “PGP” ашигласнаар та цахим орчинд өөрийгөө бүрэн илэрхийлэх, харилцагч талуудад итгэлцэл бий болгох боломжийг бүрдүүлж өгнө.

Сүүлийн үед гарч байгаа халдлагуудаас цахим шуудангаар дамжуулан хортой код, хортой холбоос зэргийг илгээж хортой код агуулсын файлыг нээх, холбоос дээр дарсан тохиолдолд

тухайн хэрэглэгчийн системийг эзэлж авдаг халдлага маш өргөн тархаад байгаа билээ. Хамгийн сүүлд гарсан том халдлага болох “Wannacry” нэртэй “ransomware” төрлийн халдлага 150 гаруй улсын 300,000 орчим сервер, компьютерт тархсан билээ. Хохирогчдын 60 хувь нь цахим шуудангаар ирсэн хортой код бүхий файл, холбоосыг нээснээс үүдэн эзлэгдсэн байх жишээтэй.

“PGP” түлхүүрийг өдөр тутмын хэрэглээнд ашиглаж хэвшсэнээр дээрхтэй ижил төрлийн халдлагуудаас бүрэн сэргийлэх боломжтой.

3. “PGP” түлхүүрийг цахим шуудан илгээхэд ашиглахгүй тохиолдолд үүсэх хор уршиг, ашигласны давуу талууд

3.1. “PGP” түлхүүрийг цахим шуудан илгээхэд ашиглахгүй тохиолдолд үүсэх хор уршиг

- Халдагч этгээд харилцагч байгууллагын албан ёсны төлөөлөгчийн цахим шууданг эзэлж түүний өмнөөс цахим шуудан илгээх
- Удирдах албан тушаалтны цахим шууданг эзэлж түүний өмнөөс хэрэгцээт мэдээллийг авах хүсэлт илгээх
- Хортой код, хортой холбоос агуулсан цахим шуудан илгээх
- Мэдээллийг дундаас нь барьж авах
- Барьж авсан мэдээллийг ашиглаж төстэй цахим шуудан, эсвэл тухайн хэрэглэгчийн цахим шууданг эзэлж хуурамч мэдээлэл илгээх
- Хөрөнгө мөнгө, эдийн засагт тодорхойлох боломжгүй хохирол учруулах гэх мэт

3.2. “PGP” түлхүүр ашиглан цахим шууданг баталгаажуулснаар доорх эрсдэлээс сэргийлэх боломж бүрдэнэ. /өдөр тутмын үйл ажиллагаанд дадал болгон ашиглах/

- Цахим шуудангийн хэрэглэгчийн нэр нууц үгээ алдсан ч “PGP” хувийн түлхүүрийн нууц үгийг алдаагүй тохиолдолд хэрэглэгчийн өмнөөс цахим шуудан илгээх боломжгүй. /2 factor authentication/
- Мэдээллийг дундаас унших, агуулгыг өөрчлөх боломжгүй болно.
- Мэдээллийн аюулгүй байдал бүрэн хангагдана.