КИБЕР ГЭМТ ХЭРЭГ БА НИЙГМИЙН ИНЖЕНЕРЧЛЭЛИЙН ТУХАЙ
CYBER CRIME AND SOCIAL ENGINEERING

Б.Ганболд, Дотоод Хэргийн Их Сургуулийн Цагдаагийн сургуулийн Гүйцэтгэх ажлын тэнхимийн багш, цагдаагийн ахмад

B. Ganbold, lecturer of the Department of Criminal intelligence at the Police School of the University of Internal Affairs, police captain

Хураангүй: Орчин үед программ хангамж үйлдвэрлэгчид программ бүтээх тал дээр илүү ур чадвартай болж, тухайн программыг эвдэж нэвтрэхэд илүү төвөгтэй болсон. Кибер гэмт хэрэгтнүүд урьдын адил программ хангамжийг эвдэн нэвтрэх, тэр дундаа алсаас нэвтрэх нь улам хэцүү болж байгаа тул нийгмийн инженерчлэлийн аргыг илүү түлхүү ашиглан, аюулгүй байдлын систем, дэд бүтцийн хамгийн сул хэсэг болох хүн рүү чиглэн довтлох болсон. Дэлхий даяар кибер гэмт хэрэгтнүүд мэдээлэл харилцаа холбооны технологийг, нийгмийн инженерчлэлийн аргатай хослуулан ашиглаж төрөл бүрийн халдлагыг үйлдсээр байна. Хэлэхэд харамсалтай ч амжилттай хэрэгжүүлсэн кибер халдлага, кибер гэмт хэрэг бүрийн ард нийгмийн инженерчлэлийн зарим нэг аргыг заавал ашигласан байдаг.

Abstract: Nowadays, software developers have become more skilled at creating software, making it more difficult to break into it. As it becomes more difficult than ever to break into software, including remote access, cybercriminals are increasingly using social engineering techniques to attack the weakest part of security systems and infrastructure: humans. Cybercriminals around the world continue to use a combination of information and communication technology and social engineering techniques to carry out a variety of attacks. Sad to say, behind every successful cyber attack and cyber crime, some form of social engineering is bound to be used.

Түлхүүр үгс: Нийгмийн инженерчэл, Фишинг халдлага, Кибер гэмт хэрэг.

Keywords: Social engineering, Phishing attack, cyber crime.

Оршил: Нийгмийн инженерчлэлийн арга гэж юу болох талаар нээлттэй эх сурвалжид "Хүмүүсийг хууран мэхлэх замаар ямар нэг үйлдэл хийлгэх, эсвэл нууц мэдээллийг задруулахад хүргэх үйл ажиллагаа юм[1]" гэж тодорхойлсон байдаг. Орчин үед нийгмийн инженерчлэл гэх энэ нэр томьёог ихэвчлэн кибер гэмт хэрэгтнүүд, хор хөнөөлтэй хакерууд ашиглаж байна. Ихэнх тохиолдолд гэмт этгээд нь хохирогчтой хэзээ ч нүүр тулдаггүйгээрээ онцлог байдаг.

[1] https://www.cisco.com

*Тэгэхээр **нийгмийн инженерчлэл** гэдэг нь амьдралын зарим нэг нөхцөл байдалд тохируулан, заль мэх ашиглан, бусдыг төөрөгдөлд оруулж эсвэл зохиомол хомсдол үүсгэн ятгаж, хүнийг сэтгэлзүйгээр нь удирдах чадвар юм*[2]. Нийгмийн инженерчлэлийн арга нь дангаараа кибер халдлага биш юм. Кибер гэмт хэргийг үйлдэхэд ашигладаг олон төрлийн халдлагын арга байдаг. Эдгээр аргуудыг үр дүнд хүрэхэд нөлөөлж байдаг гол түлхүүр арга бол нийгмийн инженерчлэлийг арга юм. Кибер халдлагыг амжилттай хэрэгжүүлэх зорилгоор кибер гэмт хэрэгтнүүд ирээдүйн хохирогч руу чиглэн хэрэгжүүлж байгаа тоглолт, заль бөгөөд үр дүнд нь хүн хамгаалалтаа бууруулж, хувийн мэдээллээ задруулах, хортой веб холбоос дээр дарах, хортой код агуулсан байж болзошгүй файл, хавсралтуудыг нээх зэрэг аюултай үйлдлийг өөрийн мэдэлгүй хийдэг.

Өөрөөр хэлбэл кибер гэмт хэрэгтэн хүмүүсийн итгэл үнэмшил, шунал дээр тулгуурлан мөрөөдөлдөө хүрэх хосгүй боломж эсвэл ямар нэг сандрал хомсдолыг зохиомлоор бий болгон бусдыг өөрийн хавханд оруулан зорилгоо хэрэгжүүлдэг. Тэд ирээдүйн хохирогчдоо маш сайн судалж, тэдний талаар жижиг гэлтгүй мэдээллийг олж өөрсдийнх нь эсрэг ашиглан итгэл үнэмшлийн олж авч, гэмт этгээдтэй харилцаанд орох зохиомол хэрэгцээ шаардлагыг бий болгодог.

НИЙГМИЙН ИНЖЕНЕРЧЛЭЛ ХЭРХЭН АЖИЛЛАДАГ ВЭ?

Кибер гэмт хэрэгтэн нийгмийн инженерчлэлийн арга ашиглан хохирогчийн таньж мэддэг хүн, бизнесийн хамтрагчийн имэйл хаяг эсвэл утасны дугаар зэргийг дуурайн харилцаанд орж албан ёсны мэт харагдах нууц үг хулгайлах зорилгоор бүтээсэн хуурамч вэб хуудас руу хөтлөх, зарим тохиолдолд итгэмжлэгдсэн байгууллагын ажилчдыг дуурайх гэх мэт арга ашигладаг. Хэрэв энэ арга заль нь үр дүнд хүрвэл (хохирогч гэмт этгээдэд итгэсэн тохиолдолд) гэмт этгээд хохирогчийг итгэл үнэмшил дээр тулгуурлан нууц үг, төрсөн огноо, банкны дансны дэлгэрэнгүй мэдээлэл гэх мэт хувь хүний нууц мэдээллийг авдаг.

НИЙГМИЙН ИНЖЕНЕРЧЛЭЛ ЯАГААД ИЙМ АЮУЛТАЙ ВЭ?

Нийгмийн инженерчлэлийн хамгийн том аюулын нэг нь халдлага үйлдэж буй гэмт этгээд хүн тус бүрд чиглэн ажиллах шаардлагагүй байдаг. Өөрөөр хэлбэл амжилттай хууртагдсан ганц хохирогч байхад л хангалттай бөгөөд түүгээр дамжуулан гэр бүл, найз нөхөд, бүхэл бүтэн байгууллагад нөлөөлж болохуйц халдлагыг хийх боломжтой байдаг. Өнөө үед нийгмийн инженерчлэлийн довтолгоонууд улам боловсронгуй болсон. Бусдын нэвтрэх нэр нууц үгийг хулгайлахаар хийгдсэн хуурамч вэбсайт, цахим шуудан нь хангалттай бодитой харагддаг төдийгүй нийгмийн инженерчлэлийн арга нь кибер гэмт хэргийн ертөнцөд хувь хүн байгууллагын хамгаалалтыг шугамыг давахад ашиглаж байгаа хамгийн түгээмэл арга нь болсон байна.

[2] Human hacking: win friends, influence people, and leave them better off for having met you, 2021.

НИЙГМИЙН ИНЖЕНЕРЧЛЭЛИЙН ХАЛДЛАГЫН ТӨРЛҮҮД

- ФИШИНГ \PHISHING\ ХАЛДЛАГА

Фишинг халдлага нь кибер орчинд хамгийн түгээмэл тархсан нийгмийн инженерчлэлийн халдлагын нэг төрөл юм[3]. Үндсэндээ фишинг гэдэг нь иргэдийн нэвтрэх нэр нууц үгийг олж авахад чиглэсэн байдаг. Хуурамч цахим шуудан ашиглах, эсвэл хууль ёсны мэт харагдах веб хуудас ашиглан бусдын нууц үгийг хулгайлдаг. Заримдаа гэмт этгээд хохирогчийг зээлийн картын мэдээлэл эсвэл бусад хувийн мэдээллээ өгөхийг албадах оролдлого хийдэг. Мөн илүү дэвшилтэт халдлагууд мөн ransomware[4] гэх мэт илүү аюултай халдлагууд ихэвчлэн фишинг халдлагаас эхэлдэг.

- УРХИДАХ ХАЛДЛАГА \WATERING HOLE ATTACKS\

Нийгмийн инженерчлэлийн энэ арга нь зорилгот бүлэг хүмүүс рүү чиглэн хэрэгжүүлдэг арга юм. Гэмт этгээд тухайн бүлэгт шууд чиглэхийн оронд тухайн бүлэг хүмүүсийн зочлох дуртай эсвэл зочлох магадлалтай веб сайтыг эвдэн дотор нь мэдээлэл олзлох хортой код бүхий урхи тавьдаг. Жишээлбэл, банк санхүү, төрийн үйлчилгээ гэх мэт тодорхой салбарын ажилтнууд байнга зочилдог тухайн салбарын вебсайтууд гэх мэт. Урхидах халдлагын хэрэгжүүлж байгаа гэмт этгээдүүд вэбсайтыг эвдэж, зорилгот бүлэг хүмүүсээс хэн нэгнийг барьж авахыг зорих бөгөөд хэрэв урхинд нэг л ажилтан орсон бол тухайн хүний дуурайн түүний хувийн мэдээлэл, имэйл хаяг, сошиал хаяг эсвэл төхөөрөмжөөр дамжуулан бусдын итгэлийг олж халдлагаа бүрэн гүйцээн зорилгоо хэрэгжүүлдэг.

- БИЗНЕСИЙН ЦАХИМ ШУУДАНГИЙН ХАЛДЛАГА \ BUSINESS EMAIL COMPROMISE ATTACKS \

Бизнесийн цахим шуудангийн халдлага гэдэг нь гэмт этгээд нь хохирогчийн удирдах албан тушаалтан, эсвэл бизнесийн түнш, ханган нийлүүлэгчдийн имэйл хаягийг дуурайлган хийж, ямар нэг данс руу мөнгө шилжүүлэхийг хүссэн, тушаасан хуурамч цахим шуудан илгээж бусдыг залилдаг бөгөөд цахим шуудан ашиглан үйлдэгддэг залилан мэхлэх гэмт хэргийн нэг төрөл юм.

- НИЙГМИЙН ИНЖЕНЕРЧЛЭЛИЙН БИЕТ ХАЛДЛАГА \PHYSICAL SOCIAL ENGINEERING \

Гэмт этгээд танай албан байгууллагад хэн нэг этгээдийн дүрд хувиран нэвтэрч халдлага үйлдэхдээ ашиглаж болох мэдээллүүдийг авах боломжтой байдаг. Албан байгууллагын туслах ажилтнууд, үүдний хүлээн авагчид, гадуур хүргэлт хариуцсан ажилтан гэх мэт эдгээр хүмүүс гэмт этгээдийн хэрэгжүүлж буй нийгмийн инженерийн биет халдлагад өртөх эрсдэлтэй байдаг. Иймд албан байгууллагууд үр дүнтэй хамгаалалттай, хяналттай байх хэрэгтэй. Жишээ нь байгууллагад ирж буй зочдыг бичиг баримттай тулган бүртгэж байх, байгууллага дотор зочдыг хяналтгүй ганцаар нь явуулахгүй байх гэх мэт.

---

[3] Руководство по защите от хакеров/ Коул Эрик. Пер. с англ. – М. Издательский дом «Вильямс», 2002.

[4] Ransomware гэдэг нь хохирогчийн төхөөрөмж дээрх файлуудыг шифрлэн түгжиж барьцаалдаг хортой вирус бөгөөд түгжээтэй файлуудыг тайлахын тулд хохирогчоос мөнгө нэхдэг.

- USB ӨГӨӨШ \ USB BAITING \

USB өгөөш нь бага зэрэг бодитой бус сонсогдож байгаа ч таны бодож байгаагаас илүү илбэг тохиолддог нийгмийн инженерчлэлийн түгээмэл халдлагын нэг юм. Кибер гэмт хэрэгтнүүд USB зөөврийн төхөөрөмж дээр хортой программ суулгаж, стратегийн чухал газруудад орхих ба хэн нэгэн сониуч ажилтан тухайн USB-г авч албан байгууллагын компьютерт залгаснаар өөрийн байгууллага руу хортой кодыг өөрөө ч мэдэлгүй оруулдаг.

ТА ӨӨРИЙГӨӨ БОЛОН БАЙГУУЛЛАГАА НИЙГМИЙН ИНЖЕНЕРЧЛЭЛИЙН ХАЛДЛАГААС ХЭРХЭН ХАМГААЛАХ ВЭ?

Нууц үг: Нууц үг бүрд байх ёстой тэмдэгтүүдийн тоо, төрлийг нэмэгдүүлэх, нууц үгийг ойр давтамжтайгаар сольж байх. Нууц үгээ хэнд ч задруулахгүй байх.

Сэжигтэй холбоос дээр дарахгүй байх: Танихгүй хүнээс сэжигтэй имэйл ирвэл нээхгүй байх. Сошиал сүлжээ ашиглан илгээсэн линк холбоос дээр дарахгүй байх. Хэрэв таньдаг хүнээс дээрх сэжигтэй тохиолдол илэрвэл биечлэн эсвэл утсаар холбогдон лавлаж байх.

Фишингийн эсрэг хамгаалалт ашиглаж байх: Олон давхар имэйл хамгаалалт нь фишинг болон бусад нийгмийн инженерийн халдлагын аюулыг багасгаж чаддаг. Зарим цахим шуудангийн аюулгүй байдлын хэрэгслүүд фишингийн эсрэг программ хангамжийг суулгасан байдаг.

Домейн нэр, линкийг шалгаж байх: Фишинг халдлагыг таних хамгийн сайн аргуудын нэг болох гипертекст холбоосыг шалгаж байх. URL холбоос нь ирсэн веб хуудастай нийцэж байгаа эсэхийг шалгаарай. Нэмж дурдахад хачирхалтай тэмдэгтүүд эсвэл товчилсон холбоосууд дээр дарахдаа болгоомжтой байгаарай. Гар утсан дээрээс орж байгаа үед та холбоос дээр дарахаасаа өмнө холбоос дээр удаан дарах үед очих URL линк жижиг цонхон дээр гарч ирэн холбоосыг ажиглаж болно. Хэрэв веб хуудсаар зочилж байгаа бол URL дээр хулганыг аваачих үед хөтчийн цонхны зүүн доод буланд линкийн очих замыг харуулдаг тул дээрх аргуудыг ашиглан линкийг \холбоос\ шалгаж болно.

Дүгнэлт: Нийгмийн инженерчлэлийн халдлага нь хүний сониуч зан, эрх мэдлийг хүндэтгэх, найз нөхдөдөө туслах хүсэл гэх мэт хүний төрөлхийн шинж чанар, нийгмийн нөхцөл байдлууд дээр тулгуурлан хүнийг төөрөгдөлд оруулахад чиглэсэн байдаг тул үүнийг эсэргүүцэн давж туулахад хэцүү байдаг. Нийгмийн инженерчлэлийн халдлагыг илрүүлэхэд туслах хэд хэдэн зөвлөмж байдаг.

Харилцаа холбоо хаанаас ирж байгааг эргэцүүлэн бодоорой; сохроор бүү итгэ. Таны ширээн дээр өмнө харж байгаагүй USB зөөврийн диск гарч ирсэн бөгөөд та энэ хэнийх болохыг мэдэхгүй байна уу? Гэнэт утсаар, эсвэл цахим шуудангаар таныг их хэмжээний мөнгө өвлөн авсан гэх мэдээ ирсэн үү? Ажлын газрын даргаас чинь яаралтай ажилчдын талаарх мэдээлэл явуулахыг хүссэн имэйл ирсэн үү? Хэрэв тийм бол эдгээр нь бүгд сэжигтэй байх тул яаран ямар нэг үйлдэл хийлгүйгээр эх сурвалжийн заавал шалгаж байгаарай.

Эх сурвалжийг шалгах нь тийм ч хэцүү биш юм. Жишээлбэл, и-мэйл ирсэн бол имэйлийн толгой хэсгийг харж, өмнө ирж байсан ижил илгээгчийн жинхэнэ имэйлтэй харьцуулан шалгана уу. Дээр дурдсанчлан холбоос хаашаа явж байгааг хараарай. Хуурамч

холбоос дээр курсороо аваачихад л хялбархан олж харна (холбоос дээр дарж болохгүй!) Үг үсгийн алдааг шалгана уу: Албан байгууллагууд өөрсдийн харилцагч үйлчлүүлэгчтэй харилцахад зориулан чадварлаг ажилчдыг ажиллуулдаг тул ямар нэг үг үсэг утга найруулгын алдаатай имэйл ирсэн бол хуурамч байж магадгүй юм.

Хэрэв та эргэлзэж байвал албан ёсны вэбсайт руу орж, албан ёсны төлөөлөгчтэй холбоо бариарай, учир нь тэд имэйл/мессеж албан ёсны эсвэл хуурамч эсэхийг баталгаажуулах боломжтой. Нийгмийн инженерчлэл нь ихэвчлэн ямар нэг яаралтай мэдрэмж түгшүүрийг бий болгосон зохиомол хомсдолыг үүсгэж байдаг. Тиймээс хэрэв танд даргаас чинь яаралтай мэдээлэл илгээхийг хүссэн имэйл ирсэн бол, эсвэл таны интернэт банкнаас таны дансанд халдлага хийхээр оролдсон байх тул яаралтай нэвтрэх нэр нууц үгээ оруулан баталгаажуулахгүй бол таны дансныг хаалаа гэсэн имэйл ирсэн бол яаран тэдний хүссэн үйлдлийг хийхээсээ өмнө нэг хором тайван бодсоноор эдгээр халдлагыг таслан зогсоож тэднийг ямар хуурамч болохыг илчлэн ирээдүйд ирэх гарз хохирлоос өөрийгөө болон дотно хүмүүсээ хамгаалж чадах юм.

Иймд утсаар мэдээлэл өгөх эсвэл холбоос дээр дарахын оронд албан ёсны дугаар руу залгаж аль эсвэл албан ёсны веб сайтын URL-аар орж шалгаарай. Мөн эх сурвалжийн найдвартай байдлыг шалгахын тулд харилцааны өөр аргыг ашигла. Жишээлбэл, хэрэв та найзаасаа мөнгө шилжүүлэхийг хүссэн имэйл, чат хүлээн авбал утас руу нь залгаж үнэхээр тэд мөн эсэхийг шалгаж байх хэрэгтэй.

Ашигласан материал:

Гүйцэтгэх ажилтан гарын авлага төсөл 2023 он
Human hacking: win friends, influence people, and leave them better off for having met you, 2021.
Руководство по защите от хакеров/ Коул Эрик. Пер. с англ. – М. Издательский дом «Вильямс», 2002.
https://www.kaspersky.com
https://www.cisco.com

Хянан магадлагаа хийсэн:

ЦС-ийн ГАТ-ийн эрхлэгч, доктор (Ph.D), цагдаагийн хурандаа Y.Хосбаяр