Использованная литература

1. Эльтазаров Б.Т., Рисхибоева Ф.Б. «Основные принципы и методы бесконтактного измерения температуры различных объектов». «Роль и задачи развития систем технологической автоматизации в разработке Республиканской научно-практической конференции» 22-23 октября 2021 г., Ферганский политехнический институт Министерства высшего и среднего специального образования Республики Узбекистан, стр. 350-352.

2. Эльтазаров Б.Т., Рисхибоева Ф.Б. «Разработка микропроцессора для бесконтактного измерения температуры». «Роль и задачи развития автоматизации технологических процессов». 22-23 октября 2021 г., Ферганский политехнический институт Министерства высшего и среднего специального образования Республики Узбекистан, стр. 353-354.

3. А.Х. Хайдаров, Ш.Абдукаримов, Б.Т.Элтазазаров., А.Эргашев. «Проектирование бесконтактных приборов измерения температуры на базе микропроцессоров», Ташкентский Государственный Технический Университет, «ЗВЕЗДЫ МАШИНОСТРОЕНИЯ» №3, 2021 г., стр. 54-56.

4. Магунов А.Н. Спектральная пирометрия, Физматлит, 2012–248 с.

5. Методы и средства бесконтактных термометров для термоконтроля и распущенности: монография / В.А. Захаренко; Мин-обр. науки России, ОмГТУ. – Омск: Изд-во ОмГТУ, 2014. – 148 с.

ТАРМОҚ ХАВФСИЗЛИГИ МУАММОЛАРИ ВА ТАРМОҚҚА ҚАРАТИЛГАН ТАҲДИДЛАР ТАҲЛИЛИ

[1]А.Т. Арзиев, [2]Р.Т.Джумамуратов, [2]Н.Р. Палуаниязова

[1]Тошкент ахборот технологиялар университети Нукус филиали,

[2]Қорақалпоқ давлат университети

Тармоқдан фойдаланиб амалга оширилувчи ҳужумлар сони ва кўринишлари жуда ҳам жадаллик билан ортиб бормоқда. Доимий ҳужумлар бутун ҳисоблаш қурилмалари дунёси учун асосий муаммодир. Шунинг учун ташкилотлар тармоқ хавфсизлигини таъминлаш учун катта харажатларни сарфлашмоқда. Тармоқ хавфсизлиги муаммолари ташкилотдаги мавжуд ахборотнинг фойдаланувчанлиги, конфиденциаллиги ва бутунлигини таъсир қилади. Ҳужумчилар технологияга тегишли хавфсизликда мавжуд бўшлиқларни аниқлашга ҳаракат қилишмоқда. Ўз навбатида бу тизим администраторида тармоқда

пайдо бўлувчи янги ҳужумлар ҳақида маълумотга эга бўлиб бориши талаб этилади.

Тармоқни қуриш осон вазифа ҳисобланиб, унинг хавфсизлигини таъминлаш мураккаб вазифа ҳисобланади. Сабаби, ҳужумчи турли воситалардан фойдаланган ҳолда тизимдаги заифликларни аниқлашга ҳаракат қилади.

Ташкилот тармоғи ичкаридан амалга оширилувчи турли ҳужумларга ҳам учраши мумкин. Ичкаридан туриб амалга оширилган ҳужум одатда ташқи ҳужумдан хавфлироқ бўлади.

Шунинг учун ташкилот кунлик тармоқдаги ҳужумларни мониторинг қилиб бориши ва аниқлаб бориши каби муҳим вазифани амалга оширишга мажбур. Ҳозирда тармоқ орқали аммалга оширилувчи муаммоларнинг ортишига қуйидаги омиллар таъсир қилмоқда:

Қурилма ёки дастурий воситани нотўғри созланиши. Хавфсизлик бўшлиқлари одатда тармоқдаги қурилма ёки дастурий воситаларнинг нотўғри созлангани боис вужудга келади. Масалан, нотўғри созланган ёки шифрлаш мавжуд бўлмаган протоколдан фойдаланиш тармоқ орқали юборилувчи махфий маълумотни ошкор бўлиши сабабчи бўлади. Нотўғри созланган қурилма ҳужумчига тизим ёки тармоқдан фойдаланиш имкониятини тақдим этиши мумкин. Нотўғри созланган дастурий восита эса илова ёки дастурий таъминдан рухсатсиз фойдалданиш имконини бериши мумкин.

Тармоқни хавфсиз бўлмаган тарзда лойиҳалаш. Нотўғри ва хавфсиз бўлмаган ҳолда лойиҳаланган тармоқ турли таҳдидларга ва маълумотни йўқотилиши эҳтимолига дуч келиши мумкин. Масалан, агар тармоқлараро экран, IDS ва виртуал шахсий тармоқ (VPN) технологиялари хавфсиз тарзда амалга оширилмаган бўлса, улар тармоқни турли таҳдидлар учун заиф қилиб қўйиши мумкин.

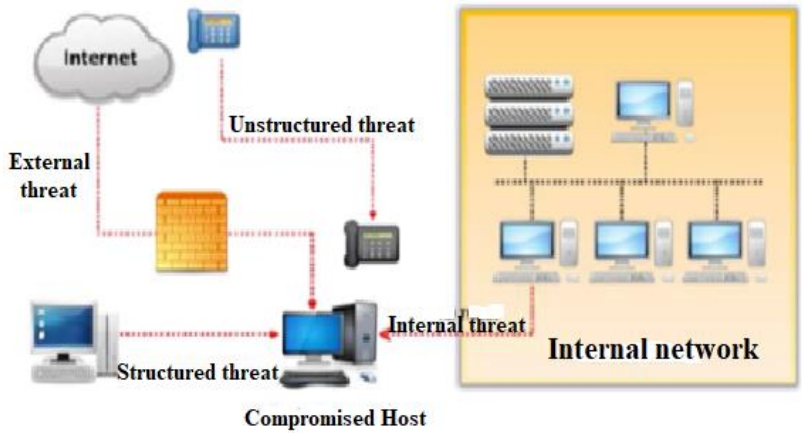
Туғма технология заифлиги. Агар қурилма ёки дастурий восита маълум турдаги тармоқ ҳужумларини бартараф эта олмаса, у ҳолда у ушбу ҳужумларни заиф бўлади. Кўплаб қурилмалар, иловалар ёки веб браузерлар *хизматдан вос кечишга ундаш* ҳужуми ёки *ўртага турган одам* ҳужумларига бардошсиз бўлади. Агар тизимларда эски веб браузер фойдаланилса, ушбу тизимлар тақсимланган ҳужумларга кўпроқ бардошсиз бўлади. Агар тизимлар янгиланмаса, кичик троян ҳужуми фойдаланувчи машинасини тозалаб ташлаш учун етарли бўлиши мумкин.

Фойдаланувчиларнинг эътиборсизлиги. Энг охирги тармоқ фойдаланувчиларининг эътиборсизлиги тармоқ хавфсизлигига жиддий таъсир қилиши мумкин. Инсон ҳаракатлари натижасида маълумотни

йўқолиши, чиқиб кетиши каби жиддий хавфсизлик муаммолари бўлиши мумкин. Бундан ташқари ҳужумчилар фойдаланувчилар ҳақида маълумотларни тўплашда социал инжинерия технологияларидан фойдаланадилар.

Фойдаланувчиларни қасддан қилган ҳаракатлари. Ишдан бўшаб кетган ходим тақсимланган дискдан ҳалигача фойдаланиш имкониятига эга бўлиши мумкин. У мазкур ҳолда ташкилот махфий ахборотини чиқиб кетишига сабабчи бўлади. Бу ҳолат фойдаланувчиларни қасддан қилган ҳаракатлари сифатида қаралади.

Тармоққа қаратилган таҳдидлар одатда икки турга ажратилади: ички таҳдидлар ва ташқи таҳдидлар.



1-расм. Турли тармоққа қаратилган таҳдидлар

Ички таҳдидлар. Компьютер ёки интернетга алоқадор жиноятчиликларнинг 80% ини ички ҳужумлар ташкил этади. Бу ҳужумлар ташкилот ичидан туриб, хафа бўлган ходимлар, ғараз ниятли ходимлар томонидан амалга оширилиши мумкин. Ушбу ҳужумларнинг аксарияти имтиёзга эга тармоқ фойдаланувчилари томонидан амалга оширилади.

Ички ҳужумлар ташқи ҳужумларга қараганда жиддий хавф туғдириши мумкин. Бунинг асосий сабаби ички ҳужумни амалга оширувчи тармоқнинг тушилиши, хавфсизлик сиёсати ва ташкилот қонунчилиги билан яқиндан таниш бўлади.

Ташқи таҳдидлар. Ташқи ҳужумлар тармоқда аллақачон мавжуд бўлган заифлик натижасида амалга оширилади. Ҳужумчи шунчаки қизиқишга, моддий фойда ёки ташкилотни обрўсини тушириш учун ушбу ҳужумларни амалга ошириши мумкин. Мазкур ҳолда ҳужумчи юқори малакали ва гуруҳ бўлиб ишлашлари мумкин. Ҳужумни амалга оширганда махсус технологиялардан фойдаланилади ва узоқ муддат давомида тайёрганлик кўрилади. Мазкур ҳолда ҳужумлар ички ходимларнинг

ёрдамисиз амалга оширилади. Баъзи ташқи ҳужумлар ўзида иштирокчиларни ва вирусга асосланган ҳужумларни, паролга қаратилган ҳужумларни, зарарли хабарни киритишга асосланган ҳужумларни ва операцион тизимга асосланган ҳужумларни ўз ичига олади.

Тармоқ хавфсизлигидаги бузилишлар қуйидаги заифликлар натижасида юзага келади:

Технологик заифликлар. Технологик заифликлар операцион тизим, принтерлар, сканнерлар ва бошқа тармоқ қурилмаларидаги камчиликларнинг натижасида юзага келади. Ҳужумчилар протоколлардаги, масалан, SMTP, FTP ва ICMP, бўшлиқларни аниқлашлари мумкин. Бундан ташқари, тармоқ қурилмалари, свитч ёки роутерлардаги аутентификация усулларининг етарлича бардошли бўлмаслиги натижасида ҳужумлар амалга оширилади. Буни олдини олиш учун, тармоқ администратори томонидан доимий хавфсизлик аудити олиб борилиши талаб этилади.

Созланишдаги заифликлар. Созланишдаги заифликлар тармоқ ёки ҳисоблаш қурилмаларини нотўғри созланиши натижасида юзага келади. Агар тармоқ администратори фойдаланувчи аккаунтини ва тизим хизматларини хавфсиз бўлмаган тарзда созланиши, жорий созланиш ҳолатида қолдириш, паролларни нотўғри бошқарилиши, натижасида заифликлар юзага келади.

Хавфсизлик сиёсатидаги заифлик. Хавфсизлик сиёсатидаги заифликни юзага келишига ташкилотнинг хавфсизлик сиёсатида қоидалар ва қарши чораларни нотўғри ишлаб чиқилгани сабаб бўлади. Ушбу сабаблар тармоқ ресурсларидан рухсатсиз фойдаланиш имкониятини тақдим этиши мумкин.

Агар тармоқ администратори ҳаракатларни доимий аудит, мониторинг қилиб борса, ушбу заифликларни аниқлаш ва ўз вақтида бартараф этиш имконига эга бўлади.

Фойдаланилган адабиётлар

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с.
2. С.К.Ганиев, М.М.Каримов, К.А.Ташев. Ахборот хавфсизлиги. –Т.: «Фан ва технология», 2016, 372 бет.
3. С.К.Ганиев, М.М.Каримов, К.А.Ташев. Ж.Т.Арзиева Информацияларды қорғаў. –Нукус.: «Каракалпакстан», 2018, 434 бет
4. Хорев П.Б. "Методы и средства защиты информации в компьютерных системах. Учебное пособие для вузов", Academia, 2008.