Урок № 10

Тема. Проблеми забезпечення безпеки в комп'ютерних системах і мережах. Типова корпоративна мережа. Рівні інформаційної інфраструктури корпоративної мережі. Мережеві загрози, вразливості і атаки. Засоби захисту мереж.

Мета:

- ✓ ***навчальна:*** ознайомитися з проблемами безпеки в комп'ютерних мережах, дати уявлення про корпоративні мережі та рівні інформаційної інфраструктури корпоративної мережі; розглянути мережеві загрози та засоби захисту мереж;
- ✓ ***розвиваюча:*** розвивати логічне й алгоритмічне мислення; формувати вміння діяти за інструкцією, планувати свою діяльність, аналізувати і робити висновки;
- ✓ ***виховна:*** виховувати інформаційну культуру учнів, уважність, акуратність, дисциплінованість.

Обладнання: комп'ютери кабінету з виходом в мережу Інтернет, мультимедійний проектор, презентація уроку, електронні матеріали.

Тип уроку: комбінований урок.

ХІД УРОКУ.

Актуалізація опорних знань

1) Давайте пригадаємо, що ви знаєте про захист інформації, пройдемо онлайн тест https://naurok.com.ua/test/start/8573 або

https://naurok.com.ua/test/osnovi-informaciyno-bezpeki-8573.html

Мотивація навчання.

Все більше і більше людей отримують доступ до мережі Internet, а хакерів і "script kiddes" на сьогоднішній день більше ніж колись. 2 листопада 1988 року був зафіксованих перший випадок появи мережевого хробака, що паралізував роботу шести тисяч інтернет-вузлів в США. Це був хробак Морріса, названий в честь автора. Збиток від нього поніс близько 96 мільйонів доларів.

Інтернет став невід'ємною частиною і постійно розвиваючою мережею, яка змінила вид діяльності багатьох людей і організацій. Багато організацій були атаковані зловмисниками, що привело до великих втрат. Мережі організацій, що не знають або ігнорують ці проблеми піддають себе великому ризику бути атакованими зловмисниками.

Ми починаємо вивчати тему «Безпека в мережі», ознайомимося із сучасними інформаційними заграми корпоративних мереж

Вивчення нового матеріалу

1. Проблеми забезпечення безпеки в комп'ютерних системах і мережах

Захист інформації в комп'ютерних системах володіє рядом специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаної з носієм, може легко і швидко копіюватись та передаватися по каналах зв'язку. Виникнення глобальних інформаційних мереж типу Internet є важливим досягненням комп'ютерних технологій, однак, з Internet пов'язано безліч комп'ютерних злочинів.

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи:

1) перехоплення інформації – при перехоплені порушується конфіденційність інформації;

2) модифікація інформації - вихідне повідомлення змінюється або повністю підміняється іншим і надсилається адресату;

3) підміна авторства інформації.

Ця проблема може мати серйозні наслідки. Наприклад, хтось може надіслати листа від вашого імені (цей вид обману прийнято називати спуфінга) або Web-сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів.

2. Корпоративна мережа.

Корпоративна мережа — це мережа, головним призначенням якої є підтримка роботи конкретного підприємства, що володіє даною мережею. Користувачами корпоративної мережі є тільки співробітники даного підприємства.

Корпоративна мережа - це складний комплекс взаємозалежних і узгоджено функціонуючих програмних і апаратних компонентів, який забезпечує передачу інформації між різними віддаленими додатками й системами, що використовуються на підприємстві.

Основними елементами мережі є робочі станції, сервери і комутатори. Основну частину мережі складають робочі станції, які підключені до комутаторів. Комутатори пересилають пакети даних з одного порту в інший за потрібною адресою. Також в мережі є сервери, що забезпечують роботу робочих станцій в складі мережі.

Наявність мережі приводить до ***вдосконалення комунікацій*** між співробітниками підприємства, а також його клієнтами і постачальниками. Мережі знижують потребу підприємств в інших формах передачі інформації, таких як телефон або звичайна пошта.

Безпе́ка мере́жі — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу.

Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів.

3. Мережеві загрози вразливості і атаки

Дії, які так або інакше загрожують збереженню, що допускають нанесення збитків інформаційній безпеці підрозділяються на певні категорії.

1. *Дії, які здійснюють користувачі, авторизовані в системі*. Ця категорія включає:
   - зловмисні дії користувача з метою крадіжки або повного або часткового знищення даних, що є на сервері або робочій станції компанії
   - пошкодження наявних даних як результат прояву необережності, халатності у діях користувача.
2. *"Електронне" втручання - дії хакерів*:
   - здійснення DOS та dDOS-атак
   - незаконне проникнення в захищені комп'ютерні мережі;

Несанкціоноване проникнення ззовні в захищену мережу тієї або іншої компанії може здійснюватися з метою нанесення збитку (знищення, підміна наявних даних), крадіжка інформації, що відноситься до розряду конфіденційною з подальшим її незаконним використанням, розпорядження мережевою інфраструктурою компанії як методом для здійснення атак на інші мережеві вузли, крадіжка грошових коштів з рахунків компанії або окремих користувачів і т.д.

Атаки категорії DOS ("Denial of Service") здійснюються ззовні і направлені на мережеві вузли тієї або іншої компанії, які відповідають за її безпечне, ефективне і стабільне функціонування (поштовий, файловий сервер). Зловмисниками організовується масова відправка яких-небудь даних на вибрані вузли, що викликає їх перевантаження, тим самим, виводячи з працездатного стану на деякий час. Подібні атаки можуть обернутися для

постраждалої компанії різними порушеннями в здійсненні безперервних бізнес-процесів, втратою клієнтів, а також втратою репутації.

3. *Комп'ютерні віруси*. Комп'ютерні віруси, так само, як і деякі інші шкідливі програми відносяться до окремої категорії способів електронної дії з подальшим нанесенням збитку. Дані засоби дії є реальною загрозою для ведення сучасного бізнесу, що має на увазі широке використання комп'ютерних мереж, електронної пошти і Інтернету в цілому. Так, "вдале" проникнення шкідливої програми (вірусу) в корпоративні мережеві вузли тягне за собою не тільки виведенням їх із стану стабільного функціонування, але і велику втрату часу, втрату наявних даних, зокрема не виключена можливість крадіжки конфіденційної інформації і прямих розкрадань грошових коштів з рахунків. Програма-вірус, яка проникла і залишилася непоміченою в корпоративній мережі дає можливість здійснення зловмисниками повного або ж часткового контролю над всією діяльністю компанії, що ведеться в електронному основним каналом для ефективного і швидкого розповсюдження спаму і вигляді.

4. *Спам*. Якщо ще кілька років тому спам був всього лише незначним по масштабах, дратівливим чинником, то в даний час технології спаму представляють достатньо серйозну загрозу для забезпечення інформаційної безпеки:

- основним каналом для ефективного і швидкого розповсюдження спаму і інших шкідливих програм стала електронна пошта;
- на перегляд спаму йде достатньо велика кількість часу, а подальше видалення численних повідомлень може викликати відчуття дискомфорту співробітників на психологічному рівні
- спам може виступати одним з основних методів реалізації різних шахрайських схем, жертвами яких можуть ставати як приватні, так і юридичні особи;
- великий ризик видалення потрібної кореспонденції разом із спамом, що може привести до різного роду неприємним наслідкам; при цьому така небезпека зростає, якщо удаватися до використання недосконалих поштових фільтрів для виявлення і відсіювання спаму;

5. *"Природні" загрози*. В категорію "природних" загроз відносять різні зовнішні чинники. Так, причиною втрати інформаційної безпеки може виступити крадіжка інформаційних носіїв, форс-мажорні обставини, неправильний спосіб зберігання інформації

Засоби захисту мереж. Політика безпеки при доступі до мереж загального значення

Для безпеки в комп'ютерних мереж використовують таке програмне забезпечення:

● Secure Shell, SSH (англ. Secure SHell — «безпечна оболонка» — мережевий протокол рівня додатків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів).

● Міжмережевий екран (брандмауер, файрвол англ. Firewall, буквально «вогняна стіна») — пристрій або набір пристроїв, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати через проксі весь комп'ютерний трафік між областями різної безпеки згідно з набором правил та інших критеріїв. Фаєрвол може бути у вигляді окремого приладу (так званий маршрутизатор або роутер), або програмного забезпечення, що встановлюється на персональний комп'ютер чи проксі- сервер.

● Антівірусна програма (антивірус) — програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом. Антивірусне програмне забезпечення складається з комп'ютерних програм, які намагаються знайти, запобігти розмноженню і видалити комп'ютерні віруси та інші шкідливі програми.

Формування практичних умінь і навичок

Увага! ***Під час роботи з комп'ютером дотримуйтеся правил безпеки та санітарно-гігієнічних норм.*** (Інструктаж з правил техніки безпеки)

Завдання 1. Ознайомитися з основними загрозами в мережі, скориставшись посиланнями: , **посилання: Zillya (Загрози в мережі Інтернет)** https://zillya.ua/zagrozi-v-merezh%D1%96-%D1%96nternet

Завдання 2. Створіть текстовий документ, що містить загальні рекомендації щодо захисту мереж.

Обговорюємо .

1. Що таке корпоративна мережа?
2. Що таке безпека мережі?
3. Які є загрози мережі, вразливості і атаки?
4. Які засоби захисту мережі?

Працюємо в парах. Які загальні рекомендації захисту мережі?

Загальні рекомендації щодо захисту мережі (від Microsoft):

- постійно інсталюйте останні оновлення для комп'ютера;
- використання брандмауера;
- запуск антивірусного програмного забезпечення на кожному комп'ютері;
- використання маршрутизатора для спільного доступу до Інтернету;
- не входьте до системи як адміністратор.

Загальні рекомендації щодо захисту мережі

- використовуйте антивірусне ПЗ;
- намагайтеся використовувати ПЗ тільки з джерел яким ви дійсно довіряєте;
- використовуйте відкрите програмне забезпечення;
- не використовуйте додатки, які визначають ваше місце положення;
- не переходіть на веб-ресурси, що здаються вам підозрілими;

Підсумок уроку

Рефлексія

- *Що нового сьогодні дізналися? Чого навчилися?*
- *Що сподобалось на уроці, а що ні? Чи виникали труднощі?*

Домашнє завдання

1) Опрацювати **конспект**,
2) За матеріалами Інтернету підготуйте бюлетень на тему: «Історія розвитку програм для захисту інформації". Розмісіть роботу на Google-диску, наддайте доступ, для перегляду і редагування учителю і 2 однокласникам. Перегляньте проектну роботу своїх друзів