НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

76-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

ТОМ 1

14 травня – 23 травня 2024 р.

УДК 369.013

А.М. Капітон, професор
О.С. Дзюбан, аспірант
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

СТІЙКІСТЬ І БЕЗПЕКА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

З розвитком інформаційних технологій та збільшенням кількості користувачів комп'ютерних систем та мереж зростає і ймовірність кібератак, які можуть призвести до серйозних наслідків, таких як витік конфіденційної інформації, порушення роботи критичних інфраструктур та навіть економічні втрати. Таким чином, забезпечення стійкості та безпеки комп'ютерних систем є актуальним завданням, що потребує розробки та застосування ефективних методів захисту.

Цифровий ландшафт – це великий і динамічний фронтир, багатий на можливості, але також таїть у собі небезпеки. Оскільки наша залежність від взаємопов'язаних технологій зв'язку, торгівлі та критичної інфраструктури продовжує зростати, зростає й уразливість до кіберзагроз. Зловмисники, від вовків-одинаків до організованих злочинних синдикатів та груп, які спонсоруються державою, постійно розробляють нові методи використання вразливостей, крадіжки даних, зриву операцій та сіяння хаосу. Потенційні наслідки успішної кібератаки можуть бути руйнівними і призвести до фінансових втрат, репутаційної шкоди та навіть фізичної шкоди.

Щоб орієнтуватися в цьому ландшафті загроз, що постійно змінюється, першорядне значення має багаторівневий підхід, який зміцнює як рівень безпеки, так і стійкість системи. В основі лежить надійна безпекова архітектура. Брандмауери діють як цифровий еквівалент рову, фільтруючи вхідний та вихідний трафік та блокуючи спроби несанкціонованого доступу. Системи виявлення та запобігання вторгненням (IDS/IPS) діють як пильні охоронці, постійно скануючи підозрілу активність у мережевому трафіку. Антивірусне та антивірусне програмне забезпечення виступає в ролі пильних вартових, постійно патрулюючи системи на наявність шкідливого коду.

Однак самі собою заходи безпеки не можуть гарантувати абсолютний захист. Кіберзлочинці невпинно шукають нові вразливості, і навіть добре захищені системи можуть бути зламані. Саме тут стійкість системи стає вирішальною лінією захисту. Під стійкістю розуміється здатність системи протистояти атакам, швидко відновлюватися після збоїв і адаптуватися до мінливих загроз.

Резервні копії даних – це цифровий еквівалент прихованого сховища, у якому важлива інформація зберігається у безпечному автономному місці. Регулярне резервне копіювання даних гарантує, що інформація не буде безповоротно втрачена у разі атаки. Надмірність системи, що досягається за

рахунок дзеркалювання критично важливих серверів та компонентів, забезпечує функцію резервного копіювання: у разі виходу з ладу одного сервера інший може легко замінити його, зводячи до мінімуму час простою та забезпечуючи безперервність бізнесу. Більше того, плани реагування на інциденти є добре відпрацьованим планом дій щодо відновлення. У цих планах викладено чіткі процедури виявлення, стримування та пом'якшення наслідків кібератак. Регулярне тестування та оновлення планів реагування на інциденти необхідні для забезпечення добре скоординованого та ефективного реагування у разі порушення безпеки.

Окрім технічних рішень, організаційна культура відіграє життєво важливу роль у побудові сильної системи кібербезпеки. Формування культури поінформованості про безпеку серед співробітників схоже на навчання жителів цифрового кордону бути пильними. Це включає навчання співробітників виявленню тактик соціальної інженерії, спроб фішингу та інших поширених кіберзагроз, надання їм можливості повідомляти про підозрілі активності і діяти в якості першої лінії захисту всередині організації. Крім того, регулярне навчання з питань безпеки дає співробітникам знання та навички для безпечної та надійної навігації у цифровому світі.

Стійкість комп'ютерної системи – це здатність протистояти різним кібератакам та зберігати працездатність навіть за умов їх здійснення. Стійкість визначається низкою факторів, включаючи архітектуру системи, якість програмного забезпечення, наявність засобів виявлення та запобігання вторгненням, а також рівень підготовки персоналу. Комп'ютерна мережа – це сукупність комп'ютерів, об'єднаних на єдину систему з допомогою різноманітних мережевих протоколів і технологій. Безпека комп'ютерної мережі полягає у забезпеченні захисту інформації від несанкціонованого доступу, спотворення, знищення та інших загроз. Забезпечення стійкості та безпеки комп'ютерних систем та мереж є складним завданням, вирішення якого потребує комплексного підходу та застосування сучасних методів захисту від кіберзагроз. Постійний розвиток інформаційних технологій та поява нових видів атак потребує постійного оновлення та вдосконалення систем безпеки, що дозволить ефективно протистояти сучасним кіберзагрозам та забезпечувати стабільну роботу комп'ютерних систем та мереж.

Постійно змінюється ландшафт загроз вимагає постійної пильності та адаптації. Команди безпеки повинні діяти як досвідчені розвідники, будучи в курсі останніх загроз, уразливостей та векторів атак, які використовуються кіберзлочинцями. Це дозволяє вживати запобіжних заходів і оновлювати протоколи безпеки для усунення ризиків, що виникають. Співпраця між організаціями, дослідниками безпеки та державними установами має вирішальне значення для обміну інформацією про загрози та розроблення колективного захисту. Уявіть собі мережу сторожових вишок, в якій кожна

організація обмінюється інформацією про загрози, що наближаються, що дозволяє забезпечити більш уніфікований захист від цифрових загарбників.\

На закінчення, безпека комп'ютерних систем та мереж у сучасному цифровому світі потребує цілісного підходу. Поєднуючи надійні заходи безпеки з практиками забезпечення стійкості систем та формуючи культуру поінформованості про безпеку, організації можуть створити надійний захист від кіберзагроз. Безперервний моніторинг, адаптація та співпраця необхідні для ефективної навігації в ландшафті кіберзагроз, що постійно змінюється, і забезпечення постійної цілісності та експлуатаційної ефективності критично важливих систем. Такий підхід дозволяє створювати безпечнішу та стійкішу цифрову екосистему для всіх.

Література

1. *В. Л. Бурячок, Р. В. Киричок, П. М. Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ: КУБГ, 2019. 320 с.*
2. *І.М. Горбаньов, О.С. Городецька. Захист інформації в комп'ютерних системах та мережах: навч. посіб. Дніпро: ДДУВС, 2020. 144 с.*
3. *О.А. Федотов. Викриття злочинів у сфері комп'ютерних: навч. посіб. Львів: НАВС, 2014. 219 с.*

УДК 519.83

Студентка групи 402 ТК С.В. Левдер
Г.В. Головко, к.т.н., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ВИКОРИСТАННЯ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ДЛЯ ПОБУДОВИ КОМП"ЮТЕРНИХ МЕРЕЖ

Бездротова мережа — комп'ютерна мережа, заснована на бездротовому принципі, що повністю відповідає стандартам для звичайних провідних мереж. Як носій інформації в таких мережах можуть виступати радіохвилі НВЧ-діапазону.

Для організації бездротової мережі в замкнутому просторі застосовуються передавачі із круговими антенами. Стандарт IEEE 802.11 визначає два режими роботи мережі як "точка-точка" - це проста мережа, в якій зв'язок між станціями встановлюється безпосередньо, без використання спеціальної точки доступу. У режимі клієнт-сервер бездротова мережа складається як мінімум з однієї точки доступу, підключеної до провідної мережі, і деякого набору бездротових клієнтських станцій. Оскільки в більшості мереж необхідно забезпечити доступ серверів, принтерів та інших