ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«Технологія захисту корпоративної мережі хостингової компанії»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Скринник В.С.
(прізвище та ініціали)
Керівник Кожуховський А.Д.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2020 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Скриннику Владиславу Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія захисту корпоративної мережі хостингової компанії»

керівник магістерської роботи Кожуховський Андрій Дмитрович, д.т.н., проф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від «10» жовтня 2020 року № 230.

2. Строк подання студентом магістерської роботи 15.12.2020 р.

3. Вихідні дані до магістерської роботи

корпоративна інформаційна система;
класифікація загроз в інформаційній безпеці;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз існуючих загроз захисту для корпоративної мережі хостингової компанії.
2. Проблеми та методи захисту корпоративної мережі хостингової компанії.

3. Засоби захисту корпоративної мережі хостингової компанії.

5. Перелік графічного матеріалу

6. Дата видачі завдання 01.10.2020 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту корпоративної мережі хостингової компанії	09.10.2020 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи	30.10.2020 р.	
3.	Аналіз існуючих загроз захисту для корпоративної мережі хостингової компанії	16.11.2020 р.	
4.	Дослідження проблем, методів та засобів захисту корпоративної мережі хостингової компанії	23.11.2020 р.	
5.	Розробка рекомендацій щодо захисту корпоративної мережі хостингової компаніїї	02.12.2020 р.	
6.	Оформлення результатів дослідження	09.12.2020 р.	
7.	Підготовка доповіді до захисту	15.12.2020 р.	

Студент _____ Скринник В.С.
(підпис) прізвище та ініціали

Керівник магістерської роботи _____ Кожуховський А.Д.
(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина магістерської роботи: 63 сторінки, 7 рисунків, 16 джерел.

Об'єкт дослідження – процес захисту корпоративної мережі хостингової компанії.

Предмет дослідження – технологія забезпечення захисту корпоративної мережі хостингової компанії.

Мета роботи – дослідити існуючи методи та засоби захисту корпоративної мережі хостингової компанії та розробити рекомендації щодо використання діючих засобів.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу забезпечення захисту корпоративної мережі хостингової компанії.

В роботі досліджено переваги і недоліки сучасних методів та засобів захисту корпоративної мережі хостингової компанії. Проаналізовані існуючі загрози інформаційної безпеки. Проведена оцінка проблем при захисті корпоративних мереж. Розроблено рекомендації щодо захисту корпоративної мережі хостингової компанії.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, МЕРЕЖА, ВРАЗЛИВІСТЬ, ЗБІЙ, АТАКА

ЗМІСТ

ВСТУП

Магістерська дипломна робота присвячена технології захисту корпоративної мережі хостингової компанії.

Корпоративна мережа – це система зв'язку, що належить одній організації та/або управляється нею відповідно до правил цієї організації.

Хостингова компанія - це компанія, що займається наданням послуг розміщення обладнання, даних і web-сайтів на своїх технічних майданчиках (хостинг).

Для співробітників, які перебувають у відрядженнях або працюють з дому, послуга віддаленого доступу до корпоративної мережі стала робочою необхідністю.

Все більше організацій дозволяють партнерам здійснювати віддалений доступ до своїх мереж з метою скорочення витрат на обслуговування систем. Тому захист кінцевих точок обміну трафіком - одна з найважливіших завдань забезпечення безпеки мережі компанії.

Місця, де корпоративна мережа підключається до Інтернету, є периметром безпеки мережі. У цих точках перетинається вхідний і вихідний трафік. Трафік корпоративних користувачів виходить за межі мережі, а інтернет-запити від зовнішніх користувачів для отримання доступу до веб-додатків і додатків електронної пошти входять в мережу компанії.

Через те, що в кінцевих точках виконується постійне підключення до Інтернету, яке зазвичай дозволяє проходження зовнішнього трафіку в корпоративну мережу, вона є основною метою атак зловмисників.

При побудові корпоративної мережі безпеки даних на кордонах мережі в точках виходу в Інтернет встановлюють міжмережеві екрани. Ці пристрої дозволяють запобігти і блокувати зовнішні загрози при проведенні термінації VPN тунелів.

Наукове завдання - дослідити існуючи методи та засоби захисту корпоративної мережі хостингової компанії та розробити рекомендації щодо використання діючих засобів.

Мета роботи – розробка рекомендацій та технологій захисту корпоративної мережі хостингової компанії.

Для досягнення мети в роботі необхідно вирішити такі завдання:

1) Провести аналіз існуючих існуючих загроз захисту корпоративної мережі хостингової компанії.

2) Дослідити методи та засоби захисту корпоративної мережі хостингової компанії.

3) Сформулювати рекомендацій щодо захисту корпоративної мережі хостингової компанії.

Об'єкт дослідження – процес захисту корпоративної мережі хостингової компанії.

Предмет дослідження – технологія забезпечення захисту корпоративної мережі хостингової компанії.

Магістерська робота складається зі вступу, трьох розділів, висновків та списку використаної літератури (16 джерел). Обсяг дослідження становить 63 сторінки. Робота ілюстрована 7 рисунками.

Тому тема магістерської роботи є актуальною.

1 АНАЛІЗ ІСНУЮЧИХ ЗАГРОЗ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ХОСТИНГОВОЇ КОМПАНІЇ

1.1. Корпоративні мережі

Корпоративна мережа – це система зв'язку, що належить одній організації та/або управляється нею відповідно до правил цієї організації. Корпоративна мережа відрізняється від мережі, наприклад, Інтернет-провайдера тим, що правила розподілу IP-адрес, роботи з Інтернет-ресурсами і т.д однакові для всієї корпоративної мережі, тоді як провайдер контролює лише магістраль мережі, дозволяючи своїм клієнтам управляти своїми мережевими сегментами, які можуть бути частиною адресного простіру провайдера, і бути прихованим механізмом мережевого перекладу адрес на одну або кілька адрес провайдера.

Мережами, як правило, керують організації, які ними володіють. Мережі приватних підприємств можуть використовувати комбінацію інтранетів та екстронетів. Вони також можуть забезпечити мережевий доступ до Інтернету, який не має єдиного власника і дозволяє практично необмежений глобальний зв’язок.

Інтранет. Інтранет - це сукупність мереж, які перебувають під контролем одного адміністративного органу. Інтранет використовує протокол IP та інструменти на основі IP, такі як веб-браузери та програми для передачі файлів. Адміністративна установа обмежує використання інтранету лише для своїх уповноважених користувачів. Найчастіше інтранет - це внутрішня локальна мережа організації. Велика інтранет, як правило, має принаймні один веб-сервер для надання користувачам організаційної інформації. Інтранет - це все, що є за маршрутизатором у локальній мережі.

Екстранет. Екстранет - це мережа, яка також знаходиться під адміністративним контролем однієї організації, але підтримує обмежене підключення до певної зовнішньої мережі. Наприклад, організація може надати доступ до деяких аспектів своєї інтранету для обміну даними зі своїми діловими партнерами або клієнтами. Цим іншим особам не обов'язково довіряти з точки

зору безпеки. Мережеве підключення до екстранету часто, але не завжди, здійснюється за допомогою технології WAN.

Міжмережева взаємодія. Міжмережева взаємодія – це здатність з'єднати комп'ютерну мережу з іншими мережами за допомогою шлюзів, які забезпечують загальноприйнятий порядок маршрутизації пакетів інформації між мережами.

Інтернет. Інтернет є найбільшим прикладом міжмережевої взаємодії. Це глобальна система взаємопов’язаних урядових, академічних, корпоративних, державних та приватних комп’ютерних мереж.

Даркнет. Даркнет - це оверлейна мережа, яка, як правило, працює в Інтернеті та доступна лише за допомогою спеціалізованого програмного забезпечення. Даркнет - це анонімна мережа, де з'єднання здійснюються лише між надійними пірами, яких іноді називають "друзями" , використовуючи нестандартні протоколи та порти.

Даркнет відрізняється від інших розподілених peer-to-peer мереж, оскільки обмін даними є анонімним (тобто IP-адреси не є загальнодоступними), і тому користувачі можуть спілкуватися, не боячись втручання уряду чи корпорації.

Незважаючи на постійні повідомлення про "хакерські атаки", які спричиняють, за публікаціями, мільярдні втрати, все більше компаній використовують Інтернет у своєму бізнесі. Добре чи погано, але це неминуче. Бізнес, який стає все більш глобальним і розподіленим, потребує єдиного середовища, єдиного простору для роботи з інформацією. І сьогодні немає альтернативи Інтернету.

На сьогоднішній день Інтернет - єдиний справді спільний простір, що дозволяє передавати, зберігати, обробляти інформацію, має добре розвинену інфраструктуру, набір дружніх протоколів та інтерфейсів і доступний майже скрізь.

Інтернет неминуче стає середовищем, завдяки якому забезпечується доступ до корпоративних даних, включаючи важливу інформацію. Коли ефективність та зручність доступу до великих обсягів даних з будь-якої точки світу стає надзвичайно важливою, вибіру не залишається. І якщо державні організації, такі

як військові чи дипломатичні установи, можуть дозволити собі використання закритих мереж, ізольованих від решти світу, комерційні організації не мають такої можливості: це невигідно, незручно і недоцільно.

У зв'язку з цим набувають все більшого поширення послуги сучасних дата-центрів, які забезпечують надійний хостинг та надають розширені можливості захисту даних. Наприклад, при дистанційній роботі з програмами за схемою ASP (оренда додатків, Application Service Provision) безпека забезпечується комплексною системою безпеки, яка включає брандмауери, сканери виявлення вторгнень, системи аудиту файлів журналів, аналіз статистики трафіку та багато іншого.

1.2. Завдання інформаційної безпеки

Завдання інформаційної безпеки (та безпеки будь-якого іншого типу), як правило, зводяться до мінімізації збитків від можливих впливів, а також для передбачення та запобігання таких впливів.

Відповідно, компонентами інформаційної безпеки є:

- виявлення об’єктів, на які можуть бути спрямовані загрози;
- виявлення існуючих та потенційних загроз;
- виявлення можливих джерел загрози;
- оцінка ризику;
- методи та засоби виявлення ворожого впливу;
- методи та засоби захисту від відомих загроз;
- методи та засоби реагування на інциденти.

Власне інформація. Її можна а) викрасти; б) знищити; в) змінити; г) заблокувати; д) скомпрометувати. Але сама по собі інформація є пасивною, щоб вплинути на неї, потрібно впливати на засіб чи систему, в якій інформація «живе». Для захисту інформації від розголошення та несанкціонованих змін в останні роки використовуються серйозно розроблені методи криптографічного захисту.

Обладнання та елементи інфраструктури. Сюди входять сервери, активне мережеве обладнання, кабельні системи, джерела живлення, допоміжні системи. Для таких об'єктів існує загроза фізичного впливу, що може призвести до пошкодження об'єкта, унеможливлення його використання або до появи в системі сторонніх об'єктів, що впливають на роботу системи або захоплення інформації. Крім того, існує ризик крадіжки об’єктів, що охороняються. Щоб мінімізувати ризик у цьому напрямку, використовуються класичні методи фізичного захисту (захисний периметр, система доступу та контроль доступу персоналу, відеоспостереження, "закладки" та сигналізація, спровоковані крадіжкою техніки, озброєною охороною, службою особистої безпеки тощо). Що стосується вірусів, які спалюють обладнання, це, на щастя, поки що лише легенда (і, можливо, питання далекого майбутнього).

Програмне забезпечення. Це операційні системи, програми, сервіси. І це основні об’єкти класичних атак та основні джерела вразливостей. Напади на такі об'єкти можуть призвести до а) краху системи (програми, послуги), часткової або повної втрати функціональності; б) здійснення стороною, що атакує (або в результаті зовнішнього впливу) несанкціонованих або непередбачених дій у системі; в) отримання контролю над системою.

Захист від атак, які використовують вразливості програмного забезпечення, як правило, є головним завданням традиційних систем захисту інформації.

Персонал. Аналіз можливостей фізичного та психологічного впливу на системного адміністратора виходить за рамки цієї статті. Хоча, серйозно кажучи про безпеку в цілому, об'єктом захисту повинен бути адміністратор великої інформаційної системи. І об'єкт пильної уваги служби безпеки. Наразі зосередимося на тому, що навмисний або випадковий вплив на персонал з адміністративними повноваженнями в системі може призвести до значних ризиків. Також зауважте, що для окремих систем "ціна запитання" може бути порівнянна з вартістю всієї системи.

Ми розглянули основні об'єкти, які піддаються загрозам з точки зору інформаційної безпеки.

1.3. Хто і що може становити загрозу для інформації? Хто може бути суб'єктом протидії таким спробам, і якими засобами можна користуватися?

"Зловмисник". Хтось із-за певних мотивів здійснює свідомі дії, які можуть завдати шкоди. Мотиви можуть бути найрізноманітнішими - від спортивного інтересу до образи роботодавця. Або до виконання службових обов'язків працівником відповідної організації.

"Адміністратор". Лояльний працівник, який має авторитет суперкористувача, який за будь-яких обставин ненавмисно вчиняє шкідливі дії. Причиною може бути основна відсутність навичок, втома, перевтома. Адміністратор має практично необмежені повноваження в системі, і навіть якщо певна інформація захищена від змін та компромісів, дуже важко запобігти її знищенню.

"Віруси". Узагальнимо під цією назвою всі «самовідтворюючі» програми, створені людиною, але багато в чому живуть власним життям, підкоряючись вкладеному в них алгоритму. Це і віруси, і хробаки, і разом з ними поширюються «троянські коні». Контроль над ними з боку творця може бути повністю втрачений або частково збережений. У випадку вірусної атаки у багатьох випадках неможливо визначити першоджерело зараження та автора програми (принаймні, це виходить за межі відповідальності та можливостей фахівців та постачальників систем захисту інформації).

Імовірність атаки, націленої на мережу хостинг-провайдера або центру обробки даних, висока. Перш за все, це пов'язано з великою кількістю виділених ресурсів. У випадку з центрами обробки даних характер опублікованої інформації, її висока вартість та важливість також стають значними. У цьому випадку ви не можете виключити небезпеку професійно підготовленої та проведеної атаки, спрямованої на отримання або знищення інформації, а також отримання контролю над ресурсом.

У випадку з "класичним" хостингом (мається на увазі компанії, які спеціалізуються на віртуальному веб-хостингу), професійна атака малоймовірна,

але навмисна кількість фронтальних атак "грубої сили", а також атак з використанням відомих вразливих місць. Напади на поштові сервери з метою безкарності за передачу великої кількості спаму (небажаної інформації, зазвичай рекламного характеру) дуже ймовірні. Що стосується складних професійних атак, їх підготовка вимагає великих зусиль (і, якщо можливо, участі інсайдерів), які будуть набагато дорожчими за результат, навіть при успішній атаці.

Політика безпеки відрізняється для різних організацій та систем. Подібно як безпека житлового будинку, магазину та атомної електростанції будується по-різному, інформаційна безпека постачальника послуг хостингу, корпоративної інформаційної системи та центру обробки даних будується по-різному.

Дата-центри, або Центри обробки даних - явище, спричинене розвитком мережі (а також розвитком бізнесу в мережі). Великі компанії, які отримують доступ до Інтернету, висувають свої вимоги насамперед до рівня надання послуг та безпеки. У той же час більшість існуючих хостингових компаній орієнтовані на інший сегмент ринку і мають свої особливості. Більшість з них не готові вирішувати подібні проблеми. Якщо повернутися до нашої метафори, то житлові будинки не призначені для розміщення промислових об’єктів та банків, а тим більше атомних електростанцій.

Хостингові компанії з'явилися раніше дата-центрів в інших економічних ситуаціях. У більшості з цих компаній головним завданням є надання недорогих і досить професійних послуг з розміщення та обслуговування веб-сайтів та простих поштових систем. Серед клієнтів - приватні особи, невеликі компанії, бюджетні організації, шоу-бізнес та багато інших. Великі корпоративні компанії та організації, пов’язані з владою та управлінням, як правило, не співпрацюють з хостинговими компаніями саме через низький рівень безпеки та негарантований рівень надання послуг.

Завдання зменшення витрат багато в чому визначає структуру інформаційної системи "класичний хостер". Як правило, використовуються небрендові сервери Linux або Free-BSD, веб-сервери Apache, бази даних MySQL та Postgress, а також скрипти Perl та PHP, всі з яких мають плюс у вигляді

безкоштовності та мінус за відсутності звичайної технічної підтримки від постачальників (однак веб-сервери Apache дійсно дуже надійні та зручні).

Слід зазначити, що у багатьох випадках "класичні" хостинг-провайдери не мають власного активного мережевого обладнання та власних каналів зв'язку, використовуючи інфраструктуру провайдера. З одного боку, це дозволяє значно знизити ціну на послуги, з іншого - позбавляє контролю та суттєво обмежує можливий рівень безпеки.

Загалом, загальний рівень захисту середнього хостера адекватний ціні розміщеної інформації та можливим загрозам. Політика безпеки зазвичай не розробляється, і всі зміни в системі вносяться одним або кількома адміністраторами. Відсутність підтримки з боку продавців, невеликий штат - все це, з одного боку, змушує системних адміністраторів завжди бути в хорошій формі, але з іншого боку серйозно знижує можливості та рівень захисту.

Дата-центри зовсім інша від хостингових компаній структура, орієнтована на надання комплексних інтегрованих послуг, які можуть знадобитися замовнику (як правило, корпоративному). Водночас однією з особливостей дата-центрів є їх висока безпека - як з точки зору охорони території, так і з точки зору технічних засобів та організаційних заходів безпеки.

Дата-центри мають свої особливості у забезпеченні інформаційної безпеки. Перш за все, це необхідність забезпечити "прозорий" доступ для клієнтів, що працюють через Інтернет (у тому числі через служби терміналів), за умови дотримання дуже суворих вимог щодо захисту інформації. Ще однією особливістю є використання різних платформ та додатків, що не дозволяє зосередити увагу на безпеці якоїсь однієї платформи або однієї товарної лінійки. Слід мати на увазі, що доступ до певної категорії інформації про клієнта не повинен мати ніхто, включаючи системних адміністраторів.

Розглянемо деякі конкретні елементи захисту, їх можливу реалізацію та доцільність застосування в різних ситуаціях.

"Нульовою" лінією захисту є приховування структури мережі, так званий захист від імітації. Спеціальне програмне забезпечення імітує сегменти мережі,

сервери та уразливості. Постійний моніторинг атак на неіснуючу мережу дозволяє виявити джерела загроз. З іншого боку, захист від імітації вводить в оману потенційних агресорів і ускладнює визначення справжньої структури системи та планування атак.

Перша лінія оборони - це детектор вторгнення IDS. Аналізуючи вхідний трафік, ця система контролює появу підписів відомих типів атак. У деяких випадках встановлюється система адаптивного захисту, в якій при виявленні певних підписів змінюються списки доступу на брандмауері. Таким чином, джерело атаки швидко блокується. Доцільно обмежити кількість перевірених підписів (що характерно, наприклад, для Cisco IDS - NetRanger). Це дозволяє підвищити продуктивність і зменшити ймовірність помилкових тривог (що є критичним для адаптивної системи). Зменшення кількості виявлених атак компенсується використанням додаткових систем виявлення вторгнень у локальних схемах захисту (найчастіше використовується вільно розповсюджуваний детектор SNORT).

Варто зазначити, що існує низка проблем із використанням IDS. Перш за все, це помилкові спрацьовування. Подібна ситуація спостерігалася під час "епідемії" Кодексу Червоного та NIMDA. Ця проблема вирішена, але завжди слід мати на увазі можливість таких подій.

У компаніях, що займаються "класичним" віртуальним веб-хостингом, апаратні IDS практично не використовуються, в першу чергу через високу вартість. Програмні «світлові» детектори також використовуються рідко, оскільки вони потребують значних системних ресурсів. Аналіз трафіку (розбір пакетів) виконується, якщо потрібно, "вручну", використовуючи такі утиліти, як tcpdump. Основна маса атак відстежується під час аналізу файлів журналів.

У дата-центрах використання як апаратного, так і програмного IDS неминуче.

Другий рівень захисту - це поділ зон безпеки, закритих мережевими екранами, і розподіл трафіку за допомогою віртуальних VLAN. Трирівневу структуру ("зовнішня зона", "демілітаризована зона" та "внутрішня зона") можна

вважати стандартним рішенням. Брандмауери - це добре описана класика. Віртуальні мережі (VLAN) у традиційному хостингу використовуються набагато рідше - головним чином через різну структуру мережі та наголос на віртуальному хостингу. Завдання ізоляції клієнтського трафіку в UNIX-віртуальних хостингових системах вирішується програмним забезпеченням.

Налаштування брандмауерів зі складною мережевою структурою є нетривіальним завданням. Взагалі використовується принцип "заборонено все, що не дозволено".

Інші методи захисту, які неминуче вимагають захисту, включають антивірусний захист. Ідеальним рішенням є централізований моніторинг антивірусів, і вибір програмного забезпечення тут досить широкий і залежить від смаку та фінансових можливостей. Що стосується антивірусного контролю пошти з автоматичним видаленням заражених повідомлень, це дещо сумнівна річ. Багато людей воліють отримувати пошту без змін. Не завжди приємно, коли антивірусна система мовчки «з'їдає» повідомлення, які містять, скажімо, підписи вірусів або повідомлення, написані про можливість атаки вірусу із прикріпленим підозрілим файлом. З іншого боку, слабкий "гігієнічний" рівень більшості користувачів та постійні атаки вірусів роблять контроль вірусів над визначеними користувачем поштовими скриньками бажаним. Принаймні, користувач повинен мати вибір, і різні типи відповідей повинні застосовуватися до різних категорій користувачів.

Аналіз журнальних файлів є невід'ємною частиною системи безпеки, незалежно від класу та рівня компанії, і зупинятися на цьому немає сенсу.

Контроль доступу та ідентифікація користувача також є невід'ємною частиною системи безпеки, яка постійно обговорюється та описується. Однак варто зосередитись на контролі доступу для адміністраторів та операторів, що мають адміністративні повноваження в системі. Постійною проблемою є генерація та зміна паролів суперкористувачем. З міркувань безпеки їх слід дуже часто міняти. Що або не відбувається, або кореневі паролі записуються на всі доступні поверхні. Хорошим рішенням є використання сучасних засобів ідентифікації та контролю доступу. Насправді фактично використовується

декілька основних методів, зокрема, на основі безконтактних елементів пам'яті Dallas Semiconductor, на основі смарт-карт (Schlumberger та подібні), а також систем біометричного контролю.

Останні (для випадку центру управління мережею дата-центрів) здаються кращими, оскільки пальці чи очі важче втратити, ніж брелок з елементом пам'яті. І є гарантія, що система включає авторизованого користувача, а не того, хто знайшов ключ.

З біометричних систем контролю найпоширенішими є сканери відбитків пальців . Ці системи, як правило, недорогі. Сканери райдужної оболонки все ще є дорогими і недостатньо надійними.

Звичайно, немає сенсу перераховувати всі технічні методи захисту.

Але слід мати на увазі, що одних лише технічних засобів, якими б потужними вони не були, недостатньо для підтримки навіть мінімального рівня безпеки.

1.4. Хостингові компанії

Хостингова компанія - це компанія, що займається наданням послуг розміщення обладнання, даних і web-сайтів на своїх технічних майданчиках (хостинг). Найчастіше, наданням послуг хостингу займаються також компанії, для яких даний вид діяльності основним не є - інтернет-провайдери, реєстратори доменів.

Завданням хостингової компанії є забезпечення доступу до обладнання або даних клієнта з Інтернету. Основними характеристиками, що визначають технічну якість послуги хостингу, є:

- Постійна доступність мережевих вузлів (так званий час роботи).
- Підключення до глобальної мережі (доступність з інших сегментів Інтернету).
- Забезпечення фізичної та інформаційної безпеки обладнання та даних.

- Забезпечення достатніх ресурсів сервера для функціонування сайту (у випадку віртуального хостингу та VDS).
- Забезпечення необхідних умов для безпечної експлуатації (електроживлення, температура повітря тощо) у разі виділення та колокації.

Хостингова компанія може надавати такі послуги:

- Розташування обладнання (colocation)
- Віртуальний виділений сервер (VDS)
- Виділений сервер(Dedicated)
- Віртуальний або спільний хостинг(shared)
- Ігровий сервер
- Сервер електронної пошти
- Інформаційне сховище даних
- Реєстрація доменних імен
- Програмне забезпечення як послуга (SaaS)
- Хмарні обчислення

Однак найпоширенішими послугами є реєстрація доменів, віртуальний хостинг, та VDS. Що це за послуги?

Доменне ім'я - символічне ім'я, яке використовується для ідентифікації областей, що є одиницями адміністративної автономії в мережі Інтернеті, як частина вищої ієрархії такої області. Кожна з цих областей називається доменом. Загальний простір імен Інтернету функціонує завдяки DNS - системі доменних імен. Доменні імена дозволяють звертатися до веб-сайтів та мережевих ресурсів, розташованих на них (веб-сайти, сервери електронної пошти, інші послуги), щоб бути представленими у зручній формі.

Віртуальний хостинг - це тип хостингу, при якому багато веб-сайтів розташовані на одному веб-сервері. Це найбільш економічний тип хостингу, придатний для невеликих проектів.

Як правило, кожен веб-сайт розміщений на власному розділі веб-сервера, але всі вони використовують одне і те ж програмне забезпечення.

Існує два основних методи доступу до веб-сайтів:

- по імені (так званим спільним IP-хостингом), коли всі веб-сайти використовують одну загальну IP-адресу.
- за IP-адресою (так званим виділеним IP-хостингом), при якій кожен веб-сайт має власну IP-адресу, а веб-сервер має кілька фізичних або віртуальних мережевих інтерфейсів.
- VDS (*virtual dedicated server*) або VPS (*virtual private server*). Віртуальний виділений сервер - послуга оренди так званого віртуального виділеного сервера. З точки зору управління операційною системою, це здебільшого відповідає фізичному виділеному серверу. Зокрема: root-доступ, власні IP-адреси, порти, правила фільтрації та таблиці маршрутизації.

Особливості VDS

На віртуальному сервері можна створювати власні версії системних бібліотек або змінювати існуючі, власник VPS може видаляти, додавати, модифікувати будь-які файли, включаючи файли в кореневому та інших каталогах служб, а також встановлювати власні програми або налаштовувати/змінювати будь-яке доступне йому прикладне програмне забезпечення.

У деяких системах апаратної віртуалізації також доступні для редагування налаштування ядра операційної системи та драйвери пристроїв.

Порівняння VPS з віртуальним хостингом

1. Кожен VPS має власну копію системи з правами доступу на кореневому рівні для Unix або Адміністратора для Windows, що дозволяє компілювати та встановлювати власне програмне забезпечення зі зміненою конфігурацією.
2. Гарантований мінімум ресурсів (пам'ять, процесорного часу).
3. Можливість архівного копіювання VPS за допомогою знімка всієї файлової системи.
4. Використання технології iSCSI дозволяє забезпечити дуже високу швидкість, а також дає можливість швидкого та зручного резервного копіювання даних.

1.5. Статистика інцидентів у хостингових компаніях

Візьмемо, наприклад, якусь середню корпоративну мережу, що містить 500 комп'ютерів з електронною поштою та доступом до Інтернету. Припустимо, що працівники мають привілеї досвідченого користувача, що дозволяє їм встановлювати програмне забезпечення та змінювати основні налаштування комп’ютера. Вважається, що електронна пошта проходить через корпоративний поштовий сервер, захищений одним з найпопулярніших антивірусів у нашій країні, таким як AVP або DrWeb, а доступ до Інтернету здійснюється централізовано через корпоративний проксі-сервер та брандмауер. У цьому випадку статистика випадків має вигляд, показаний на рис. 1.

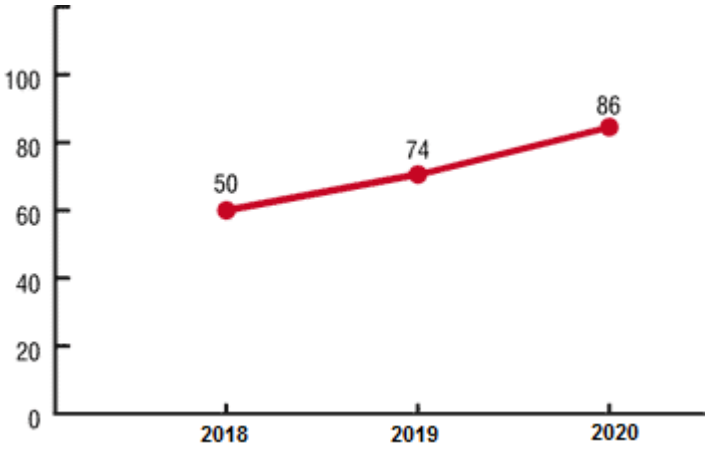

Рис.1 .1. Статистика випадків

Зрозуміло, що це середня статистика щодо якоїсь міфічної мережі, як і в будь-якій реальній локальній мережі, ці цифри можуть бути різними, оскільки вони залежать від багатьох факторів. Аналіз причин інцидентів показує картину, зображену на рис. 2.

Рис. 1.2.Схема причин інцидентів

Як видно зі схеми, основною причиною різного роду інцидентів є шкідливі програми різного типу. Ця категорія включає віруси, шкідливе програмне забезпечення (шпигунське програмне забезпечення, модулі розміщення реклами та інше небажане програмне забезпечення). Дуже часто поява шкідливого програмного забезпечення безпосередньо пов'язана з діями користувача, такими як відвідування веб-сайтів або встановлення невиробничих програм.

На схемі, показаній на рис. 1.2., видно, що приблизно 25% інцидентів спричинені діями користувачів, і інцидент може трапитися у разі навмисних дій (які передбачають наявність у користувача мережі локальної мережі зловмисних намірів і план його реалізації) або ненавмисний. Аналіз показує, що переважна більшість випадків, пов'язаних із користувачами, спричинені навмисними діями. Решта 5% потрапляють до категорії, що називається хакерськими атаками, а хакерська атака включає використання інструментів соціальної інженерії.

Чого компанії бояться і як справи йдуть насправді?

Щорічно проводяться опитування, щоб визначити ставлення IT-фахівців до питань інформаційної безпеки. Дослідження показали, що переважна більшість компаній недооцінюють кількість шкідливих програм, які існують сьогодні. Більше того, вони навіть не припускають, що кількість шкідливих програм постійно збільшується.

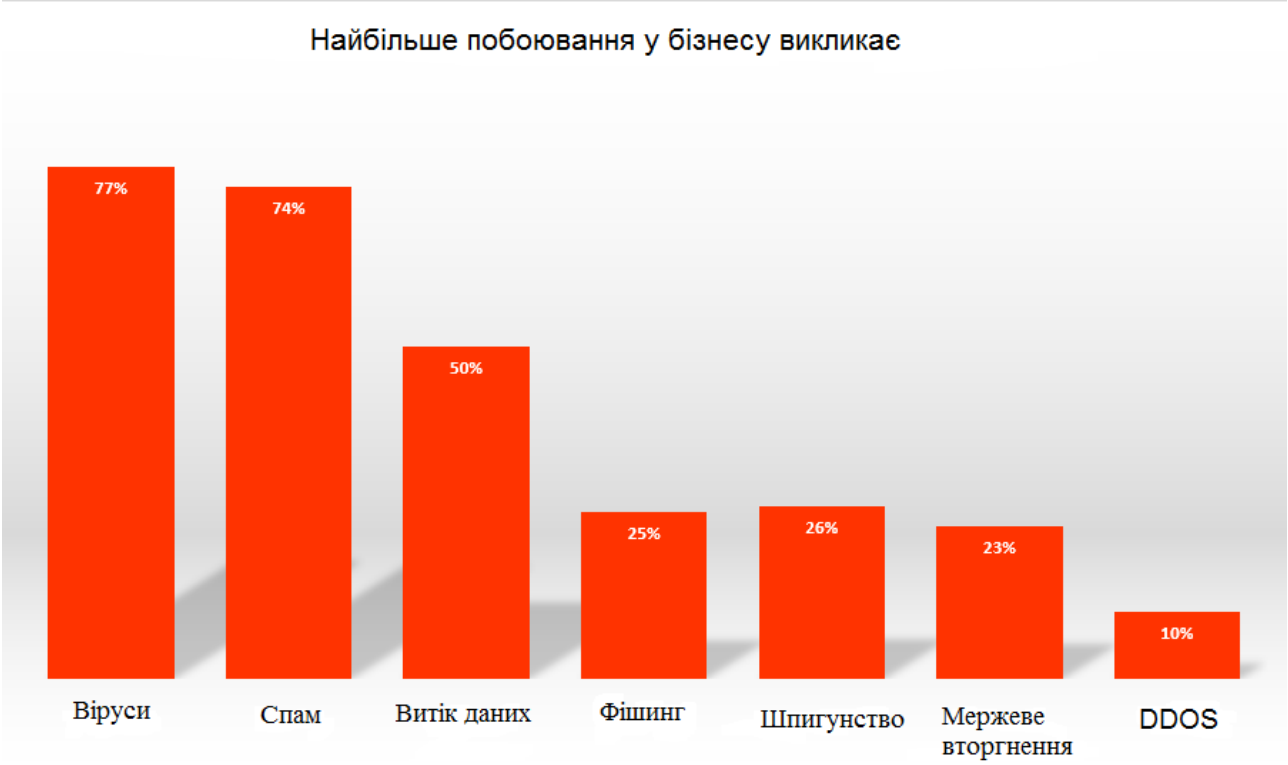

Рис. 1.3. Схема найбільшої загрози, очами компаній

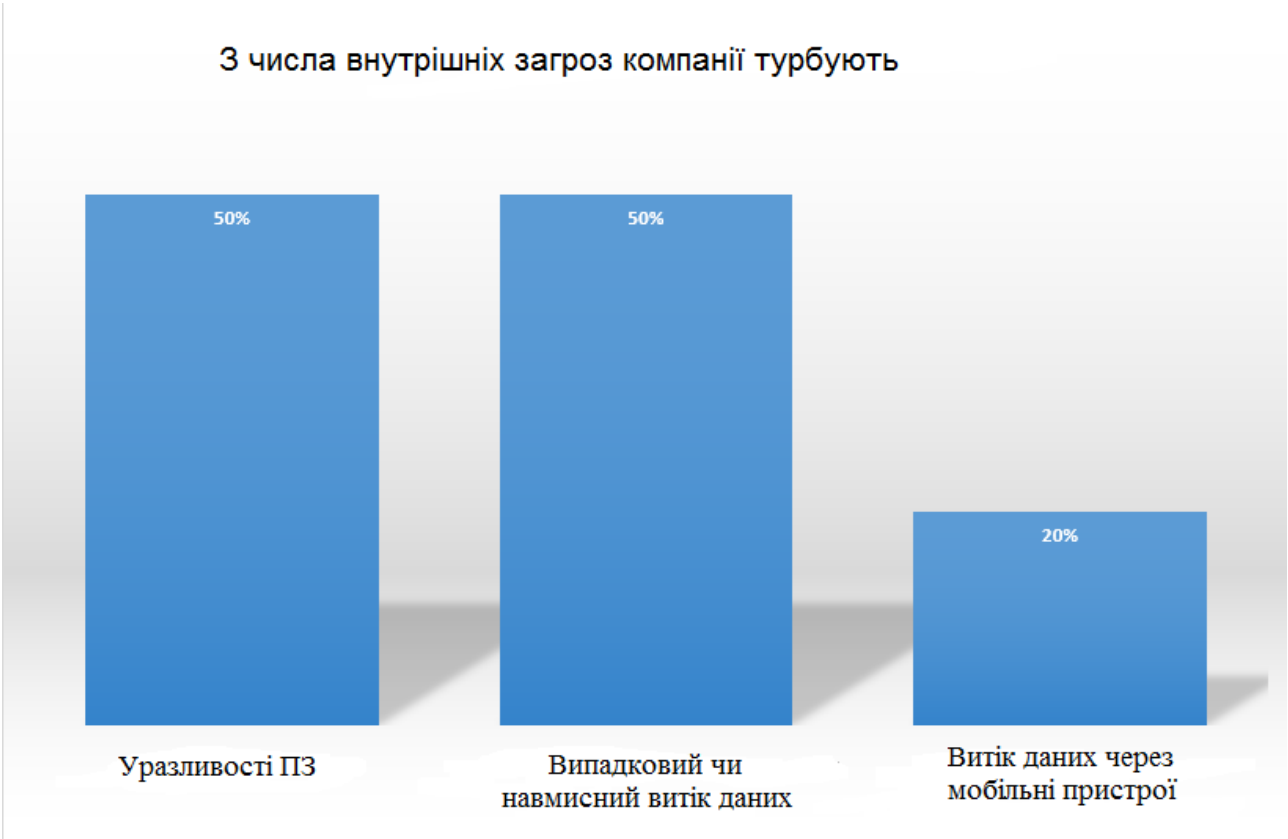

Рис.1.4. Схема найбільших внутрішніх загроз, очами компаній

Цікаво, що приблизно 13% IT-спеціалістів кажуть, що вони не хвилюються про внутрішні загрози.

Це може бути пов’язано з тим, що деякі компанії не ділять кіберзагрози на зовнішні та внутрішні. Крім того, серед керівників служб IT та ІС є і ті, хто все-таки надають перевагу вирішуванню всіх проблем з внутрішніми загрозамизабороняючими заходами.

Однак якщо людині заборонено щось робити, це не означає, що вона цього не робить. Тому будь-яка політика безпеки, включаючи заборону, вимагає відповідних засобів контролю, які забезпечать відповідність усім вимогам.

Що стосується типів інформації, які в першу чергу представляють інтерес для зловмисників, як показали дослідження, сприйняття компаній та реальний стан справ дуже різні.

Так, самі компанії найбільше бояться ватратити:

- інформацію про клієнтів;
- фінансові та операційні дані;
- інтелектуальну власність.

Трохи менше бізнес турбується про:

- інформацію по аналіз діяльності конкурентів;
- платіжну інформцію;
- персональні дані працівників;
- дані про корпоративні банківські рахунки.

Насправді виявляється, що кіберзлочинці частіше усього крадуть внутрішню операційну інформацію компаній.

1.6. Організація захисту інформації в корпоративній мережі малого та середнього бізнесу

Як правило, малі організації обмежуються використанням автоматичних фільтрів електронної пошти та стандартних антивірусів (часто неліцензійних), здатних мати справу лише з найневиннішими шкідливими програмами . Для того, щоб сьогодні знайти «інфекцію» в Інтернеті, не потрібно виконувати ніяких хитромудрих дій, все дуже просто. У зв’язку з цим ситуація набагато

небезпечніша, ніж кілька років тому, оскільки сучасні віруси можуть потрапляти на комп'ютер після того, як користувач виходить в мережу, не чекаючи, поки він натисне небезпечне посилання. Але, звичайно, крім них, існує багато загроз для корпоративних даних. Хакери можуть підключитися до системи, або інформація може бути знищена внаслідок несправності обладнання або помилки працівника.

Рис.1.5. Схема загроз корпоративної мережі малого та середнього бізнесу

ІТ-загрози для малого та середнього бізнесу. Чим вища важливість інформаційних технологій для підприємства, тим ретельніше слід захищати дані. Запобіжні заходи слід застосовувати регулярно, але не втручатися у бізнес-процеси. І звичайно, потрібно дотримуватися «золотої середини», уникаючи таких ситуацій:

Позиція 1. «Щоб муха не літала». Існує шифрування абсолютно будь-яких корпоративних даних, використання програм працівниками здійснюється під найсуворішим контролем, працівникам заборонено користуватися Інтернетом і т. д. Звичайно, ніщо не може порушити цілісність і конфіденційність інформації в такій фірмі. Однак незабаром бізнес зруйнується, оскільки персонал не зможе ефективно працювати в таких умовах. Крім того, захист цього рівня вимагає величезних витрат на його впровадження та обслуговування системи.

Позиція 2. "Зараз не в безпеці". Облікові записи не захищені паролем, будь-який відвідувач має необмежений доступ до даних, що зберігаються на комп'ютерах співробітників, виявлення вірусів - звичайна подія. Така організація не тільки втратить довіру клієнтів (їх контакти будуть швидко ідентифіковані конкурентами та запропонуватимуть вигідніші умови), але й ризикуватиме серйозними фінансовими втратами в разі шахрайства з боку банківської системи.

Щоб цього не сталося, попросіть керівників різних підрозділів компанії сказати вам, які засоби будуть для них найбільш корисними та чому. На основі отриманих даних ви зможете уявити загальну ситуацію на даний момент в організації та вжити необхідних заходів для забезпечення безпеки корпоративних мереж.

Загрози, зокрема в галузі IT, поділяються на кілька великих груп за ступенем частоти їх виявлення та масштабом можливих негативних наслідків:

1. Висока загроза - велика шкода. Якщо у компанії склалася така ситуація, вона зможе позбутися проблем, лише якщо раніше створила резервну копію важливих файлів.
2. Висока загроза - невеликий збиток. Для усунення неприємностей не потрібно робити нічого особливого.
3. Низька загроза - велика шкода. Хорошим заходом захисту тут було б отримати страхування заздалегідь, щоб компенсувати збитки.
4. Мала загроза - невеликий збиток. Ви можете ігнорувати такі випадки.

Як показує практика, у понад 80% випадків інформація потрапляє в руки зловмисників через неписьменність або неуважність працівників. І лише в останні 20% крадіжка корпоративних даних здійснюється навмисно. Якщо причиною аварії стали неправильні дії персоналу, навіть найсучасніші системи захисту можуть бути безсилі. Тому важливо розповісти працівникам про можливі наслідки їхньої недбалості та пояснити, як діяти далі. Це допоможе позбутися більшості потенційних загроз.

Робота з працівниками. Вже зазначалося, що персонал часто винен у витоках даних корпоративної мережі. Звичайно, це не завжди навмисно. Одна справа, якщо вашу клієнтську базу виснажує програміст 1С конкурента. І інша справа, якщо секретар, розповідаючи знайомому про місце роботи, згадав, що запланована зустріч із іноземним інвестором. Щоб зменшити кількість таких випадків, необхідно працювати з працівниками: Поясніть, яку інформацію корпоративної мережі не можна виносити з офісу, як влаштована система, яких дій слід уникати, невідповідність загрожує бізнесу, і т. д. Підвищення лояльності персоналу до компанії. З цією метою справляються різні мотиваційні програми.

І те, і інше однаково важливо. В іншому випадку працівники будуть або неписьменними, або навмисно ігноруватимуть стандарти безпеки.

Висновки до першого розділу

1. Проведено аналіз існуючих загроз захисту корпоративної мережі хостингової компанії, в результаті були визначені основні види кіберзагроз та причини їх виникнення.
2. Досліджена статистика інцидентів в хостингових компаніях.
3. Проведено аналіз організації захисту інформації в корпоративній мережі малого та середнього бізнесу**.**

2 ДОСЛІДЖЕННЯ ПРОБЛЕМ, МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ХОСТИНГОВОЇ КОМПАНІЇ

2.1. Проблеми захисту інформації

Проблеми інформаційної безпеки є одними з найважливіших у побудові надійної інформаційної системи на базі ПК. Ці проблеми включають як захист від несанкціонованого доступу до даних, так і фізичний захист даних цих та системних програм, особливо захист від комп'ютерних вірусів. Таким чином, поняття захисту даних включає збереження цілісності даних та контроль доступу до даних (авторизація).

Для найбільш ефективного використання засобів захисту даних, що використовуються на практиці, їх включення повинно передбачати використання ПК у службі на ранній стадії. Слід підкреслити, що організація інформаційної системи, заснованої на локальній мережі та ПК з жорсткими дисками, має серйозний недолік: всі загальні процедури фізичного обмеження доступу до ПК стають неефективними, а проблемний центр переходить до організації контролю за колективним використанням даних. Таким чином, для колективного використання залишається проблема захисту особистої інформації кожного користувача.

Проблема збереження цілісності цих даних має організаційний та технологічний аспекти.

Організаційний аспект включає наступні правила: розміщення та встановлення ПК повинно виключати можливість безконтрольного їх використання та перегляду інформації особами без доступу; завантаження загального та спеціального програмного забезпечення без засобів розмежування доступу дозволяється, якщо ПК не має доступу до локальної мережі і не має жорстких дисків (при наявності жорстких дисків ПК використовується одним користувачем або всі користувачі мають рівні повноваження); носії даних (дискети) повинні зберігатися у особи, відповідальної за роботу ПК, у місцях, недоступних стороннім особам, і видаватися користувачам лише в робочий час;

важлива інформація повинна мати кілька примірників на різних носіях; захист даних на жорсткому диску повинен підтримуватися періодичним копіюванням на дискети та розподілом пам'яті жорсткого диска на кілька розділів, які розподіляються між користувачами; дані, що стосуються різних завдань, доцільно зберігати окремо; він повинен суворо керуватися правилами поводження з магнітними носіями; контроль за доступом до ПК здійснює особа, відповідальна за його роботу; всі роботи, що виконуються на ПК, повинні бути записані в журнал реєстрації та запевнені користувачем та особою, відповідальною за експлуатацію.

Технологічний аспект пов'язаний з різними типами обмежень, які підтримуються структурою бази даних, що використовується в інформаційній системі, і повинні бути доступними для користувача. До них належать: обмеження поновлення певних атрибутів з метою збереження необхідних пропорцій між їх старими та новими значеннями; обмеження, що вимагають збереження значень поля індикатора в певному діапазоні; обмеження, пов'язані із зазначеними функціональними залежностями. Зазвичай в СУБД мовою маніпулювання даними вже закладені її компоненти зазначених обмежень.

Проблеми захисту від комп'ютерних вірусів безпосередньо пов'язані з проблемами захисту інформації від несанкціонованого доступу.

Для їх створення створено велику кількість програмного забезпечення. Хтось із них займається шифруванням інформації, хтось - обмеженням доступу до даних.

Частина вірусів постійно знаходиться в пам’яті комп’ютера, частина виробляє руйнівні дії одним «ударом». Існує також цілий клас програм, які виглядають цілком пристойно, але насправді псують систему. Такі програми називаються "троянські коні".

Однією з головних властивостей комп’ютерних вірусів є здатність до "розмноження" - тобто саморозмноження всередині комп’ютера та комп’ютерної мережі.

Оскільки різні офісні програми змогли працювати з програмами, написаними спеціально для них (наприклад, для Microsoft Office ви можете писати програми на Visual Basic), з’явився новий тип шкідливого програмного забезпечення - так звані макровіруси.

Віруси цього типу поширюються разом із звичайними файлами документів і містяться в них як звичайні підпрограми.

Як віруси, дії яких є руйнівними (знищення даних або операційна система), так і троянські програми можуть бути поширені. Троян - програма, яка непомітно працює на зараженому комп'ютері і надає зловмисникові різні опції: отримання файлів паролів поштою, віддалене управління, виведення повідомлень тощо.

Враховуючи потужний розвиток засобів зв'язку та різко збільшений обмін даними, проблема захисту від вірусів стає дуже актуальною.

Проблема фізичного несанкціонованого доступу до інформації зараз є досить актуальною.

Несанкціоновані дії на комп'ютері користувача стають можливими завдяки наявності дірок у різних компонентах програмного забезпечення.

Найчастіше потрібно стежити за буфером. Поширеною вразливістю є її переповнення. За відсутності перевірки правильності або довжини будь-яких параметрів занадто велике значення параметра в оперативній пам'яті виходить за межі виділеного йому буфера і записується поверх виконуваного коду. Навіть коли запущений звичайний користувач, процеси з вищими привілеями запускаються в операційній системі.

Отже, виконання несанкціонованого коду залежить від рівня, на якому виконується вразливий процес.

Виконання довільного коду та завантаження файлів на атакований комп'ютер може здійснюватися за допомогою компонентів ActiveX, вбудованих у HTML-код об'єктів, компонентів, що використовують зовнішні програми (наприклад, Media Player). У кожній версії програмних продуктів Microsoft є добре відомі уразливості, навіть з усіма встановленими пакетами оновлень та виправлень. Тому не можна сподіватися, що розробники забезпечать безпечну

взаємодію всіх різноманітних програмних продуктів, технологій та модулів операційної системи.

Через специфічні налаштування за замовчуванням виникає досить багато вразливостей. Для їх усунення досить змінити конфігурацію програмного забезпечення, яке утворилося в результаті його встановлення. Перш за все, вам слід або відключити виконання різних сценаріїв Java, сценаріїв та додатків, виконання та завантаження елементів ActiveX, використання файлів cookie або, принаймні, налаштувати свої програми так, щоб усі ці дії виконувались лише після явного дозволу користувача .

У внутрішньокорпоративній діяльності певна кількість інформації повинна зберігатися на комп'ютері у доступній формі для постійної роботи з ним, що створює джерело витоку під час фізичного доступу до даних.

Методи простого шифрування даних не зручні, оскільки для роботи з інформацією її все одно доведеться розшифрувати. Однак існують методи, які дозволяють зробити це швидко і непомітно для користувача (прозоро), тому створюється враження роботи зі звичайними даними.

Існують також методи «гарячого» захисту критичної інформації. Уявіть ситуацію: існує загроза фізичного доступу до інформації (наприклад, спроба викрасти комп'ютер). У цьому випадку працівник відділу режиму натискає спеціальну кнопку, і зловмисник потрапляє в руки комп'ютера, на якому «немає» інформації. Після повернення комп'ютера до нормальної роботи за допомогою спеціального ключа у вигляді брелка або пластикової картки вся інформація відновлюється у початковому вигляді.

Проблема фізичного доступу до інформації. Однак проблема фізичного доступу до інформації сьогодні не є основною.

Проблеми захисту інформації в мережі. У будь-якому випадку необхідно захищати мережу або ділянку мережі від вторгнення ззовні, зберігаючи доступ зсередини. Для таких цілей існує брандмауер. Зараз розроблено багато брандмауерів, і просто придбати один з них недостатньо.

По-перше, кожен брандмауер має свої переваги та недоліки. По-друге, вам потрібно правильно налаштувати брандмауер і контролювати його роботу в майбутньому. І по-третє, у корпоративній мережі можуть бути конкретні завдання, пов'язані з видом діяльності, для яких необхідно спеціально налаштувати брандмауер, щоб вони не заважали один одному і одночасно не давали канали витоку інформації.

Однак головним у вирішенні мережевих проблем захисту інформації є наявність інформаційної системи, яка відповідає наступним вимогам:

1. Однорідна комп'ютерна мережа, заснована на найсучасніших версіях операційних систем сімейства Windows.
2. Грамотна конфігурація брандмауерів відповідно до політики, прийнятої компанією (організацією). Постійна підтримка відповідності цього параметра прийнятій політиці.
3. Регулярне автоматичне оновлення компонентів операційної системи сервера та клієнта.
4. Централізоване використання та оновлення програмного забезпечення проти зловмисного програмного забезпечення (антивірусного, антиспамового та шпигунського програмного забезпечення).
5. Використання інфраструктури відкритих ключів , включаючи: мережі CA, шифрування пошти, електронний цифровий підпис. Обов'язкове формування сертифікатів на смарт-картках (токенах).
6. Використання політики безпеки для облікових записів користувачів та IPSEC на рівні доменної структури локальної мережі.
7. Використання програмного від централізованого контролю доступу для запису інформації на зовнішні носії через порти та пристрої COM, LPT, USB, FireWire, IrDA, CD / DVD-RW тощо.
8. Організація фізичного захисту серверів і робочих станцій: контроль доступу та відеоспостереження в серверній кімнаті, закриття корпусів ПК замками.
9. Використання моніторингу та швидкого реагування на вразливості та порушення інформаційної безпеки: контроль електронної пошти та HTTP-

трафіку, сканери проникнення, внутрішні аналізатори безпеки операційних систем, системи виявлення та запобігання вторгненню (IDS / IPS).

Цей перелік вимог не є повним. Це лише найважливіші «цеглинки» системи захисту інформації, які зменшують ймовірність порушень (витік або пошкодження інформації, або відмова у доступі до систем), а також умови їх виникнення (умови виникнення означають такі зараження шкідливим програмним забезпеченням, дірки в програмному забезпеченні, несанкціоноване встановлення та запуск програм, можливість несанкціонованого запису інформації на зовнішні носії або її несанкціоновану розсилку поза локальною мережею тощо).

Проблема захисту інформації в Інтернеті. Інтернет став чудовим середовищем для дослідників-самоучок (хакерів). Хоча статистика показує, що 80 відсотків порушень безпеки відбуваються всередині компаній, чи то злочини щодо керівництва працівників, зловживання чи нехтування владою.

Майже всі організації вже переступили межу, коли корпоративна мережа обмежувалася простором однієї будівлі. Філії або замовники організацій та установ можуть знаходитись на будь-якій відстані один від одного. І єдиним зручним, доступним і дешевим засобом спілкування був Інтернет.

Відразу виникає проблема захисту інформації під час її проходження через Інтернет. Для реалізації захищеного каналу даних із використанням відкритих (незахищених) мереж зв'язку була розроблена концепція віртуальних приватних мереж (VPN). Ця концепція включає методи ідентифікації та авторизації клієнтів, аутентифікацію та контроль цілісності (незмінності) переданих даних, захист інформації, що передається від несанкціонованого доступу криптографічними методами, що забезпечує рівень безпеки, достатній для розширення корпоративних мереж за допомогою Інтернету .

За допомогою технології VPN будь-яка компанія зможе вийти на ринок, який раніше вважався недосяжним для потужностей компанії, працюючи з клієнтами через Інтернет абсолютно безпечно.

На цьому етапі розвитку інформаційних технологій відбувається поступове витіснення паперового документообігу на електронне практично в організаціях будь-яких сфер діяльності. Однак, маючи незаперечні переваги, це нововведення "грішить" і недоліки, вимагаючи, наприклад, захисту переданих електронних документів.

Найгостріше питання захисту документів відчувається в організаціях, які мають географічно розподілену структуру та глобальні загальнодоступні комп'ютерні мережі, такі як Інтернет. А його використання для передачі даних є найнебезпечнішим через величезну кількість користувачів. Адже серед них знайдуться ті, кому інформація, передана вами або для вас, буде надзвичайно корисною!

Загрози таких користувачів можна розділити на дві основні категорії. Загроза конфіденційності інформації, тобто несанкціонований доступ до документів. А загроза цілісності інформації - можливі спроби змінити в процесі передачі електронний документ або нав'язати неправдиву його версію під виглядом юридичної. Відповідно, існує два основних методи захисту від таких загроз: шифрування для забезпечення конфіденційності електронних документів та електронних підписів для забезпечення цілісності та точності авторства документа.

Інтеграція світового інтернет-співтовариства проходить швидкими темпами. Все більше людей отримують шанс отримати заражену вірусом електронну пошту, і все більше клієнтів електронної пошти готові поширювати вірус.

Кожні шість місяців, а то й частіше з'являється вірус, який б'є всі попередні рекорди або за швидкістю, і за масштабом. Хороший вірус генерує безліч модифікацій, часто небезпечніших за вихідну версію. Слід зазначити, що віруси схильні до складних розчинів. Інтегрований підхід використовується як для розповсюдження, так і для несприятливих наслідків.

Проникнення здійснюється не просто через поштовий клієнт або браузер, але також через IRC, або навіть через негерметичний сервер від Microsoft - Internet Information Server, а також це для комп'ютерів, які відвідують заражений

сайт. І деструктивні прояви вірусу - це вже не просто знищення даних або заповнення вільного місця на диску.

Черв'ячний вірус BadtransII не тільки викрадає паролі для віддалених та мережевих з’єднань, але й відстежує натискання клавіш та надсилає файл LOG на певну електронну адресу.

Гучний Інтернет-хробак Nimda, крім заповнення мережевих дисків сміттям, також відкриває загальний вміст дисків зараженого комп'ютера та надає користувачеві "Гість" права адміністратора.

Тож найближчим часом необхідно підготуватися до появи вірусів, які атакують систему з різних сторін і використовують кілька різних помилок у програмному забезпеченні, наприклад багатофункціональний інтелектуальний шкідливий ПЗ. І оскільки плакати до свідомості вірусів абсолютно марно, вам слід просто дотримуватися основних заходів безпеки, особливо щодо файлів, які надходять до вас через всесвітню павутину.

2.2. Методика побудови корпоративної системи захисту інформації

Головною метою будь-якої системи інформаційної безпеки є забезпечення стійкої роботи об'єкта: запобігання загрозам його безпеці, захист законних інтересів власника інформації від незаконних посягань, включаючи злочинні дії в цій сфері відносин, що забезпечує нормальну виробничу діяльність усіх підрозділів об'єкта. Іншим завданням є підвищення якості послуг, що надаються, та гарантій захисту майнових прав та інтересів клієнтів6.

Для цього потрібно:

- віднести інформацію до категорії обмеженого доступу (службова таємниця);
- прогнозувати та своєчасно виявляти загрози безпеки інформаційних ресурсів, причини та умови, що сприяють фінансовій, матеріальній та моральній шкоді, порушенню їх нормального функціонування та розвитку;

- створити умови функціонування з найменшою ймовірністю реалізації загроз безпект інформаційних ресурсів та заподіяння різного роду збитків;
- створити механізм та умови для швидкого реагування на загрози інформаційній безпеці та прояву негативних тенденцій у функціонуванні, ефективного припинення посягань на ресурси на основі правових, організаційних та технічних заходів та засобів безпеки;
- створити умови для максимально можливої компенсації та локалізації шкоди, заподіяної незаконними діями фізичних та юридичних осіб, і тим самим зменшити можливий негативний вплив наслідків порушень інформаційної безпеки.

Рис.2.1. Схема захисту інформації

На рис.2.1. Представлена схема захисту інформації , яка являє собою сукупність об’єктивних зовнішніх та внутрішніх факторів та їх впливу на стан

інформаційної безпеки на об’єкті та на збереження матеріальних чи інформаційних ресурсів.

Розглядаються такі об'єктивні фактори:

- загрози інформаційній безпеці, які характеризуються ймовірністю виникнення та ймовірністю реалізації;
- вразливості інформаційної системи або системи контрзаходів (систем захисту інформації), що впливають на ймовірність реалізації загрози;
- ризик - фактор, що відображає можливу шкоду організації в результаті загрози інформаційної безпеки: витік інформації та її неправильне використання (ризик в кінцевому рахунку відображає ймовірні фінансові втрати - прямі чи непрямі).

Для побудови збалансованої системи захисту інформації планується спочатку провести аналіз ризиків інформаційної безпеки. Потім визначають оптимальний рівень ризику для організації на основі зазначених критеріїв. Система захисту інформації (контрзаходи) повинна будуватися таким чином, щоб досягти заданого рівня ризику.

Запропонований метод аналітичної роботи дозволяє повністю проаналізувати та задокументувати вимоги, пов'язані з інформаційною безпекою, уникнути витрат на непотрібні заходи безпеки, можливі при суб'єктивній оцінці ризиків, надати допомогу в плануванні та здійсненні захисту на всіх етапах життєвого циклу інформаційних систем, забезпечити виконання робіт у стислі терміни, надати обґрунтування вибору контрзаходів, оцінити ефективність контрзаходів, порівняти різні варіанти контрзаходів.

При побудові моделі враховуватиметься взаємозв'язок між ресурсами. Наприклад, вихід з ладу будь-якого обладнання може призвести до втрати даних або відмови іншого важливого елемента системи. Такі відносини визначають основу побудови моделі організації з точки зору ІС.

Ця модель, згідно із запропонованою методологією, будується наступним чином: для виділених ресурсів визначається їх величина, як з точки зору пов'язаних з ними можливих фінансових втрат, так і з точки зору шкоди репутації організації, дезорганізації її діяльності, моральна шкода від розголошення конфіденційної інформації тощо. Потім описується взаємозв'язок ресурсів, виявляються загрози безпеці та оцінюється ймовірність їх реалізації.

На основі побудованої моделі ви можете обґрунтовано вибрати систему контрзаходів, що знижує ризики до прийнятних рівнів і має найвищу економічну ефективність. Частиною системи контрзаходів будуть рекомендації щодо регулярних перевірок ефективності системи захисту.

Забезпечення підвищених вимог до ІС забезпечує відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Планування цих заходів здійснюється після завершення етапу аналізу ризику та вибору контрзаходів. Обов’язковою частиною цих планів є періодична перевірка відповідності існуючого режиму ІБ політиці безпеки, сертифікація інформаційної системи (технології) на відповідність вимогам певного стандарту безпеки.

2.3. Формування політики організаційної безпеки

Перш ніж пропонувати будь-які рішення щодо інформаційної безпеки, слід розробити політику безпеки. Політика організаційної безпеки визначає процедуру надання та використання прав доступу користувачів, а також вимоги до звітування користувачів про їх дії у питаннях безпеки. Система захисту інформації (ITS) буде ефективною, якщо вона надійно підтримує імплементацію правил політики безпеки, і навпаки. Етапи побудови організаційної політики безпеки - полягає у включенні в опис об'єкта автоматизації структури вартості та аналізі ризиків та визначенні правил для будь-якого процесу використання цього типу доступу до ресурсів об'єкта автоматизації, які мають такий ступінь вартості.

Політика організаційної безпеки складається у вигляді окремого документа, який узгоджується та затверджується Замовником.

Перш за все, необхідно зробити детальний опис загальної мети побудови охоронної системи об’єкта, що виражається через сукупність факторів або критеріїв, що конкретизують призначення. Сукупність факторів є основою для визначення вимог до системи (вибір альтернатив). Фактори безпеки, у свою чергу, можна поділити на юридичні, технологічні, технічні та організаційні.

Вимоги гарантії досягнутого захисту виражаються через оцінку функцій безпеки NIB об'єкта. Оцінка сили захисної функції проводиться на рівні окремого механізму захисту, і її результати дозволяють визначити відносну здатність відповідної охоронної функції протистояти виявленим загрозам. Виходячи з відомого потенціалу атаки, сила захисної функції визначається, наприклад, категоріями "основний", "середній", "високий". Потенціал нападу визначається шляхом вивчення можливостей, ресурсів та мотивів зловмисника.

Перелік вимог до системи захисту інформації, ескізного проекту, плану захисту (далі - технічна документація, ТД) містить набір вимог безпеки до інформаційного середовища об'єкта, які можуть посилатися на відповідний профіль безпеки, а також містити чіткі вимоги.

Загалом, розробка ТД включає:

- уточнення захисних функцій;
- вибір архітектурних принципів будівництва NIB;
- розробка логічної структури NIB (чіткий опис інтерфейсів);
- роз'яснення вимог функцій забезпечення гарантії NIB;
- розробка методів і програм випробувань на відповідність сформульованим вимогам.

На етапі оцінки досягнутої безпеки проводиться оцінка заходів щодо забезпечення безпеки інформаційного середовища. Гарантійний захід заснований на оцінці, з якої після впровадження рекомендованих заходів можна довіряти інформаційному середовищу об'єкта. Основні положення цієї техніки

передбачають, що ступінь гарантії випливає з ефективності зусиль при проведенні оцінки безпеки. Збільшення зусиль з оцінки включає:

- значна кількість елементів інформаційного середовища об’єкта, що бере участь в процесі оцінки;
- розширення типів проектів та описи деталей виконання при проектуванні системи забезпечення безпеки;
- строгість, що полягає у використанні більшої кількості інструментів та методів пошуку для виявлення менш очевидних вразливостей або для зменшення ймовірності їх присутності.

2.4. Загальні методи захисту корпоративної інформації

З точки зору інформаційної безпеки, "слабкою ланкою" і найбільш вірогідною внутрішньою загрозою є користувач, який регулярно отримує доступ до ресурсів та даних у корпоративній мережі. Згідно з дослідженням IBM та Ponemon Institute2, у 74% випадків фатальну роль відігравала помилка користувача. Тому ми залишатимемо поза увагою несправність та поломку обладнання, вірусні епідемії, захист від хакерських атак, інспекцію дорожнього руху, аналіз журналів та інші методи протидії технологічним загрозам. Зосередьтеся на користувачі як на головній загрозі.

Підвищення обізнаності користувачів. Чому користувачі помиляються? Найчастіше - через незнання та необережність. Стабільність системи захисту інформації прямо пропорційна обізнаності та відповідальності користувачів. Навчайте працівників, змушуйте їх - буквально - вивчати правила роботи з конфіденційною інформацією, виключати можливість отримання привілеїв «неофіційно», минаючи правила безпеки. Поясніть ступінь серйозності збитків у разі необережності чи незнання, покладіть на працівників особисту відповідальність, включаючи фінансову.

Моніторинг прав доступу. Перш за все, необхідно провести аудит для визначення рівнів доступу та сценаріїв роботи користувачів з документами та файлами.

У невеликих фірмах розуміння ієрархії користувачів та рівнів доступу підпорядковується пояснювальному системному адміністратору. Він має достатньо стандартних інструментів для моніторингу привілеїв та управління правами доступу до всіх ресурсів та програм.

Для моніторингу прав середніх компаній краще використовувати централізовані інструменти, які сканують корпоративну мережу і автоматично виявляють зловживання або потенційно небезпечні дії користувачів з інформацією. Таким інструментом є, наприклад, SIEM-системи.

Великі компанії рекомендують ще глибшу автоматизацію аудиту прав за допомогою спеціалізованих інструментів IDM. Впровадження та обслуговування IDM-рішень часто є унікальним процесом, який враховує специфіку конкретної галузі та кожного замовника.

Основний принцип моніторингу, неважливо в «ручному» або автоматизованому режимі - щоденний аудит усіх об'єктів доступу. Мета полягає в тому, щоб обмежити можливість користувачів створювати нові об'єкти самостійно та уважно стежити за змінами в правах доступу до вже створених об'єктів. Інакше одного разу на комп’ютері секретаря з’явиться загальнодоступна папка з річним фінансовим звітом.

Великі компанії рекомендують більш глибоку автоматизацію аудиту прав за допомогою спеціалізованих інструментів IDM, ніж для середнього та малого бізнесу. Впровадження та підтримка IDM-рішень часто є унікальним процесом, який враховує специфіку конкретної галузі та кожного замовника.

Диференціація прав доступу. Наступним кроком є «скорочення» прав: чим менше можливостей у користувача для навмисних або випадкових порушень, тим вищий ступінь захисту інформації. Розподілу прав передують дві важливі процедури.

Спочатку потрібно скласти список законних власників важливої інформації в компанії. По-друге, чітко регламентувати обов'язки працівників, визначати ресурси та документи, необхідні для безперебійного робочого процесу. Наприклад, якщо бухгалтер залишається без доступу до трекера завдань відділу розробки і не бачить, які завдання перелічені у відділі технічної підтримки, робота бухгалтерії не зупиниться. Якщо інженеру заборонено доступ до адміністративної частини корпоративного сайту для редагування новин, процес розробки продукту не постраждає.

Вибір інструментів для розмежування прав доступу - це «питання смаку». Для цього підходять засоби Active Directory, веб-сервіси та вбудовані опції додатків - будь-який сучасний IT-продукт надає можливість так чи інакше організувати рівні доступу.

Важливо лише те, що розмежування прав користувачів у корпоративній екосистемі набуває якості циклічної роботи. У міру розвитку компанії зміни у бізнес-процесах або кадровому забезпеченні неминуче з’являються у користувачів з недостатніми або, навпаки, надлишковими правами. Тому аудит і розподіл ролей слід проводити регулярно.

Шифрування

Будь-яка корпоративна мережа завжди має важливу інформацію, яка недостатньо захищена обмеженням доступу до неї. Найпростіший і найочевидніший приклад - особисті дані працівників. Криптографія забезпечує додатковий захист конфіденційних даних.

Шифрування - це простий і доступний метод захисту інформації. Він забезпечує безпечну передачу даних всередині компанії та через Інтернет, коли співробітники надсилають інформацію через мережу, наприклад, обмін документами через файловий сервер або надсилання електронних листів. Шифрування також захищає від фізичних загроз, включаючи крадіжку або втрату ноутбуків, підключаються пристроїв та зовнішніх носіїв інформації. У кожній із цих ситуацій зашифровані дані марні для зловмисників.

Спектр криптографічних інструментів варіюється від вбудованих інструментів операційної системи та апаратних мережевих пристроїв для шифрування трафіку до шлюзів шифрування каналів зв'язку та спеціалізованих інструментів шифрування, таких як шифрування баз даних.

Практично всі алгоритми шифрування, що використовуються у продуктах ВТ, є надійними та здатними захищати дані. Різниця, безумовно, присутня, але в реальному житті це не має значення. Дані, зашифровані навіть найпростішими способами криптографії, в більшості випадків залишаться недоступними для зловмисників.

Ще одна особливість методу шифрування пов’язана з впливом на швидкість робочих процесів. Захоплення шифруванням уповільнює роботу, наприклад, використання надмірно криптостійких алгоритмів при копіюванні інформації на флешку може зайняти у користувача в 2-3 рази більше часу, ніж використання класичних алгоритмів.

Адекватне шифрування означає вибір на користь невидимого, швидкого алгоритму без об'єктивних ризиків розкриття даних. З точки зору бізнесу, нерозумно сповільнювати роботу компанії за допомогою складних криптографічних алгоритмів лише для того, щоб зловмисники витратили не десятки, а сотні років на розшифровку. Тому інформація в кінцевих точках часто зашифрована або не надто складне спеціалізоване програмне забезпечення, або вбудовані засоби Windows.

При всіх своїх перевагах шифрування не захищає від головної внутрішньої загрози - людського фактора. Користувачі мають доступ до ресурсів та "ключів" із зашифрованих файлів. Щоб захистити корпоративну інформацію від інсайдерської діяльності, вам потрібно перейти до аналізу вмісту.

Адекватне шифрування означає вибір на користь невидимого, швидкого алгоритму без об'єктивних ризиків розкриття даних. З точки зору бізнесу, ірраціонально сповільнювати роботу компанії за допомогою складних криптографічних алгоритмів лише для того, щоб зловмисники витратили не

десятки, а сотні років на розшифровку. Тому інформація в кінцевих точках часто шифрується або не дуже складним спеціалізованим програмним забезпеченням, або вбудованими інструментами Windows.

Контактний аналіз

Контактний аналіз відповідає на питання, з якою інформацією працює користувач і чи є ця інформація (конкретний документ чи файл) критичною для компанії.

Для цього вам потрібно «інвентаризувати» файли та документи, що зберігаються у спільних папках та жорстких дисках комп'ютерів користувачів, баз даних, корпоративних NAS (мережеве сховище), SharePoint, веб-серверів та інших IT-об'єктів. Потрібен інструмент, який виявлятиме обмежену інформацію в будь-якому «покинутому куточку» корпоративної інфраструктури. Це завдання краще за інших вирішується DLP-системами з функцією управління даними "в стані спокою" (Data at Rest).

Захист конфіденційної інформації - це циклічний процес, який більше залежить від організаційних, а не технічних методів. Навчання користувачів правилам інформаційної безпеки, моніторингу та розмежування прав доступу, шифруванню даних, впровадженню DLP-системи - всі ці методи забезпечують надійний захист лише за розумного та всебічного підходу. Грамотне поєднання основних методів може значно підвищити безпеку корпоративних даних та запобігти самій можливості випадкового витоку даних або навмисного розкриття конфіденційної інформації.

2.5. Справжні приклади випадків у корпоративній мережі, пов'язаних із діями користувачів

Розглянемо кілька типових випадків, які чітко демонструють типові випадки, пов'язані з діяльністю користувачів. Усі описані нижче випадки взяті з практики і з дуже високим ступенем ймовірності можуть мати місце в будь-якій корпоративній мережі.

Випадок 1. Багаторівневе закачування

Сценарій. Працівник К завантажує з Інтернету утиліту для багатопотокового збереження контенту зазначених сайтів. Після вказівки декількох сайтів вона запускає утиліту у фоновому режимі. В результаті несправності утиліта починає видавати 500-700 запитів в секунду безперервно, що призводить до ситуації DoS на корпоративному проксі-сервері.

Аналіз. У цьому випадку зловмисний намір з боку працівника відсутній, але аналіз ситуації показав, що використання цієї утиліти не потрібне для вирішення виробничих проблем. Крім того, утиліта не пройшла жодних тестів адміністраторами мережі і її використання не було узгоджено з ними, що, власне, призвело до такої ситуації.

Рішення проблеми. Політика корпоративної безпеки забороняє встановлювати програмне забезпечення, яке активно взаємодіє з Інтернетом, без згоди адміністраторів та служб безпеки. Після цього вживаються технічні заходи

Випадок 2. Електронна пошта

Сценарій. Бажаючи привітати колег з Новим роком, працівник К складає базу розсилки з 1500 адрес, потім створює лист із Flash-мультфільмом розміром в 1,5 Мбайт і запускає розсилку.. Подібні операції виконують його колеги, надсилаючи вітальні листівки із вкладеними картинками, флеш-кліпами та звуковими файлами. В результаті на поштовому сервері створюється DoS-ситуація, а прийом та надсилання ділової кореспонденції блокується.

Аналіз. Це типовий приклад зловживання корпоративною електронною поштою, зазвичай подібні проблеми виникають перед святами. Така ситуація найбільш характерна для великих мереж (понад 500 користувачів).

Рішення проблеми. Технічно цю проблему вирішити дуже складно, оскільки обмеження обсягу електронних листів та кількості електронних листів за одиницю часу не завжди є прийнятними та неефективними при великій кількості користувачів. Найефективнішим заходом є розробка правил використання корпоративного поштового сервера та доведення цих правил до відома всіх користувачів.

Випадок 3. Інструменти для мережевого аналізу

Сценарій. Нещодавно найнятий молодий програміст для самоосвіти завантажує сканер мережевої безпеки XSpider з Інтернету. Для вивчення своєї роботи він встановлює налаштування по максимуму і в якості цілі вказує адресу одного з корпоративних серверів. Як результат, засоби захисту сервера реєструють атаку, уповільнюючи час реакції сервера на запити користувачів.

Аналіз. У цьому випадку відсутній зловмисний намір, оскільки встановлений цією програмою користувач мережі не мав чіткого уявлення про можливі наслідки.

Рішення проблеми. Політика корпоративної безпеки вводить розділ, який суворо забороняє встановлювати та використовувати на робочому місці користувачів активних та пасивних інструментів дослідження мережі, генераторів мережевих пакетів, сканерів безпеки та інших інструментів. Відповідно до цього положення, використання таких інструментів дозволяється лише адміністраторам мереж та спеціалістам з інформаційної безпеки.

Випадок 4. Поштовий вірус

Сценарій. Користувач отримує лист, що містить очевидні аномалії (відправником та одержувачем листа є сам користувач, текст листа не відповідає діловій кореспонденції або відсутній). До листа додається архів із деяким додатком. Незважаючи на інструктаж, інтерес сильніший, користувач зберігає архів на диск, розпаковує та запускає файл, який виявляється новим типом поштового хробака.

Аналіз. Технічні заходи в цьому випадку марні. Той факт, що користувач отримав лист, свідчить про те, що застосований антивірус електронної пошти та антивірус на ПК користувача не виявляють цей тип вірусу.

Вирішення проблем. Навчання користувачів та розробка планів дій на випадок появи пошти або мережевого хробака в корпоративній мережі.

Випадок 5. Несанкціоноване підключення модему

Сценарій. Користувач несанкціоновано підключає стільниковий телефон до свого комп’ютера та отримує доступ до Інтернету через з’єднання GPRS. Під

час роботи в Інтернеті на його комп'ютер заходить комп'ютерний хробак, який потім намагається заразити інші комп'ютери всередині локальної мережі.

Аналіз. Стільникові телефони з GPRS дуже поширені, тому організувати несанкціонований пункт підключення не складно. Небезпека такого підключення дуже велика, оскільки воно не контролюється адміністраторами і не захищене корпоративним брандмауером.

Рішення проблеми. Існує два шляхи вирішення цієї проблеми: технічний та адміністративний. Для ефективного захисту слід застосовувати обидва: з одного боку, політика корпоративної безпеки повинна суворо забороняти користувачам підключати модеми чи стільникові телефони до Інтернету, а з іншого - вживати технічних заходів для блокування цієї можливості (привілеї безпеки та політики, інструменти моніторингу).

Випадок 6. Заражений ноутбук

Сценарій. Користувачеві надається службовий ноутбук, який він бере з собою у відрядження. Там він підключається до мережі, і його комп'ютер заражається комп'ютерним хробаком. Повернувшись, він підключається до локальної мережі, і його ноутбук стає джерелом зараження мережі.

Аналіз. Така ситуація є досить поширеною, тобто в цьому випадку вірус потрапляє в мережу, підключившись до мережі зараженого мобільного комп'ютера (ноутбука, КПК). Проблема посилюється наявністю сучасних ноутбуків Wi-Fi адаптерів.

Рішення проблеми. Ця проблема не має однозначного рішення. Хороші результати досягаються установкою антивіруса та брандмауера на ноутбук, а установку виконують адміністратори, і користувачеві категорично заборонено їх відключати або переналаштовувати.

Випадок 7. Робота з електронною поштою в обхід корпоративного поштового сервера

Сценарій. Користувач запускає одну або кілька поштових скриньок в Інтернеті та використовує їх для обходу корпоративного поштового сервера. В

результаті він отримує лист з вірусом, а згодом його комп'ютер стає джерелом зараження локальної мережі.

Аналіз. Це досить поширена ситуація. Захистити корпоративний сервер досить просто, встановивши систему поштових фільтрів та антивірусів (як варіант - кілька антивірусів). В обхід поштового сервера відкривається порушення мережевої безпеки, яке не контролюється адміністраторами. Вищезазначене також стосується мережевих комунікацій, таких як ICQ, MSN Messanger та їх аналогів.

Рішення проблеми. Найефективнішим рішенням є заборона співробітникам компанії використовувати сторонні поштові скриньки. З одного боку, цей крок здається жорстким заходом, з іншого - закриває канал витоку інформації та усуває одне з основних джерел проникнення шкідливих програм у мережу.

2.6. Засоби захисту корпоративних мереж хостингових компаній

Говорячи про систему захисту інформації корпоративної мережі, ми маємо на увазі виконавців та заходи, які вони вживають. В даний час розроблені спеціальні правила, написані нормативні акти та розпорядчі документи, які диктують, які інструменти та технології слід використовувати для запобігання витоку даних.

Наявність надійної системи захисту корпоративних мереж гарантує безпеку даних та захищає від несанкціонованого втручання в роботу компанії ззовні. Говорячи про це, слід розуміти, що мова йде про захист на випадок не тільки хакерських атак, але і банальної неуважності працівників, недовговічного «апаратного забезпечення», недоліків програмного забезпечення та інших факторів, прояв яких неможливо передбачити.

Правильно організований захист корпоративних мереж - це багаторівнева автоматизована система, що включає безліч елементів, які постійно взаємодіють між собою. Повинен бути план дій на випадок виходу з ладу будь-якого з цих

компонентів з будь-якої причини, ризик якої, звичайно, є. Всі компоненти такої системи поділяються на кілька основних категорій:

1. Пристрої. Це слово стосується персональних комп’ютерів, що використовуються в процесі роботи, та їх компонентів, а також зовнішніх пристроїв (наприклад, принтерів, накопичувачів, кабелів тощо).

2. Придбане програмне забезпечення. Сюди входять всілякі системні програми, завантажені програми, утиліти тощо.

3. Інформація. Дані, які можна зберігати по-різному: на магнітних носіях, у друкованому вигляді тощо.

4. Фахівці. Співробітники компанії безпосередньо відповідають за роботу всієї системи, а також користувачі зв’язуються з нею.

Автоматизована система захисту має певний набір специфічних особливостей. Зокрема, це виражається в тому, що будь-які системні суб'єкти та об'єкти, а також засоби масової інформації мають свій електронний аналог.

1. Засоби, за допомогою яких інформація може надаватися в тій чи іншій формі: різні носії інформації, файли, зовнішні пристрої (принтери, термінали тощо), внутрішня пам’ять комп’ютера тощо.

2. Об'єкти системи відіграють у ній пасивну роль. Їх призначення полягає лише у тому, щоб служити "провідниками" даних, дозволяючи їм передавати їх з однієї точки в іншу. У зв'язку з цим кожен об'єкт містить певний обсяг інформації. Ви можете отримати доступ до вмісту, лише порушивши його.

3. Суб'єкти системи - це, навпаки, активні елементи. Вони можуть впливати на систему, викликаючи різні зміни в ній. Вони також визначають, яку інформацію та куди надсилати. Суб'єктами є користувачі, деякі програми або процеси.

Безпека даних досягається лише тоді, коли всі компоненти системи працюють разом і є цілісним механізмом, а інформація залишається надійною та конфіденційною.

Ступінь необхідності захисту даних безпосередньо залежить від останнього. Чим більше вони секретні, тим ретельніше їх слід захищати (наприклад, коли йдеться про персональні дані клієнтів компанії, банківські реквізити тощо).

Тільки уповноважені організації мають право працювати з конфіденційною інформацією корпоративної мережі, яка перевіряється кожного разу, коли ви входите в систему, підтверджуючи ваш дозвіл у ній. Це стосується не лише людей, а й різних програм та процесів. Суб'єкти, не зареєстровані в системі, не мають доступу до інформації корпоративної мережі.

Висновки до другого розділу

1. Дослідженні проблеми захисту корпоративної мережі хостингової компанії.
2. Дослідженні методи захисту корпоративної мережі хостингової компанії.
3. Проведено аналіз випадків у корпоративній мережі, пов’язаних із діями користувачів.
4. Дослідженні засоби захисту корпоративної мережі хостингової компанії.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ХОСТИНГОВОЇ КОМПАНІЇ

3.1. Практичні поради щодо поліпшення захисту

Для безпеки не менш важливо враховувати не тільки технології та системи, а й враховувати людський фактор: розуміння цілей професіоналів, які будують систему, та розуміння відповідальності працівників, які використовують пристрої.

Останнім часом зловмисники все частіше покладаються не лише на технічні засоби, але і на слабкі сторони людей: вони використовують методи соціальної інженерії, які допомагають отримати майже будь-яку інформацію.

Працівники, переносячи дані на своєму пристрої, повинні розуміти, що вони несуть точно таку ж відповідальність, як якщо б носили з собою паперові копії документів.

Персонал компанії також повинен добре знати, що будь-який сучасний технічно складний пристрій містить дефекти, якими може скористатися зловмисник. Але щоб скористатися цими дефектами, зловмисник повинен мати доступ до пристрою. Тому, завантажуючи пошту, програми, музику та картинки, потрібно перевірити репутацію джерела.

Важливо з обережністю ставитися до провокаційних SMS та електронних листів і перевіряти надійність джерела перед тим, як відкривати лист та переходити за посиланням.

Для того, щоб компанія все ще мала захист від таких випадкових або навмисних дій працівників, вона повинна використовувати модулі для захисту даних від витоків.

3.2. Розробка нормативних документів

Як зазначалося під час аналізу типових проблем, що виникають у локальній мережі підприємства, багато з них не можуть бути вирішені суто технічними засобами - необхідний набір внутрішньокорпоративних нормативних документів.

Основними є положення про комерційну таємницю та положення про захист інформації.

Положення про комерційну таємницю. Положення про комерційну таємницю є основним документом, в якому зазначається, яка інформація вважається комерційною таємницею фірми. Цей документ зазвичай містить кілька типових розділів:

- загальні положення - тут розміщена вступна частина та посилання на закони, на яких базується це положення;
- основні поняття комерційної таємниці - детальне тлумачення всіх термінів і понять, включаючи інформацію, що становить комерційну таємницю, ноу-хау, режим комерційної таємниці, носіїв комерційної таємниці;
- захист комерційної таємниці - це сукупність заходів та методів, які використовуються або можуть використовуватися організацією для захисту комерційної таємниці. У цьому розділі зазвичай описується процедура отримання доступу до комерційної таємниці та покарання за її розголошення;
- перелік відомостей, що становлять комерційну таємницю;
- особливі обов'язки осіб, допущених до комерційної таємниці та відповідальних за охорону комерційної таємниці.

З точки зору захисту корпоративної мережі, останні два пункти представляють інтерес. По-перше, все, що стосується структури локальної мережі, використовуваних засобів захисту та конфігурації цих засобів, має бути оголошено інформацією категорії "суворо конфіденційна". Відповідно, розділ про відповідальність осіб, допущених до комерційної таємниці, повинен описувати процедуру підключення користувача до ресурсів, що містять інформацію, що становить комерційну таємницю. Ідеальний варіант - розробити уніфіковану програму підключення, яка схвалена службою безпеки та безпосереднім керівництвом користувача. У цій заявці ви можете надати графу, яку повинен заповнити IT-фахівець, із зазначенням дати надання доступу. Ведення таких

заявок з їх реєстрацією та нумерацією дозволяє встановити суворий порядок надання доступу до інформації.

Після розробки та затвердження положення про комерційну таємницю розробляється другий документ - положення про захист інформації.

Положення про захист інформації. Цей документ повинні розробляти IT-спеціалісти (або спеціалісти з безпеки за участю фахівців з інформаційних технологій). Цей документ регулює роботу користувачів у корпоративній мережі та встановлює їх права та обов'язки. Ідеологічно положення про захист інформації базується на положенні про комерційну таємницю. Типове забезпечення інформаційної безпеки може містити чотири основні моменти:

- загальні положення, що описують мету документа та його склад;
- вимоги до процесу розробки та впровадження програмного забезпечення власної розробки - регулюють відносини між розробниками програмного забезпечення та адміністраторами і описують вимоги до програмного забезпечення з точки зору інформаційної безпеки;
- вимоги до стороннього програмного забезпечення - тут, крім фактичних вимог, потрібен опис процедури експертизи та процедури її проведення;
- обов'язки персоналу щодо забезпечення режиму інформаційної безпеки при роботі комп'ютерів, мережевих комунікацій та програмного забезпечення - це основний розділ, де детально регламентовані всі правила поведінки користувачів у мережі, використання програмного та апаратного забезпечення. Крім того, цей розділ регулює взаємодію між користувачем та адміністраторами;
- дії посадових осіб у разі порушення режиму інформаційної безпеки - розділ містить покрокову схему, що описує порядок дій у разі надзвичайних ситуацій або порушень режиму безпеки. Крім того, у цьому розділі описано, як відключити користувача від наданих йому мережевих ресурсів у разі порушень.

Після розробки положення про захист інформації воно повідомляється всім працівникам під розписку та призначаються працівники, відповідальні за контроль за дотриманням затвердженого положення. Практика показує, що дуже гарні результати досягаються у випадку формалізації процедури надання доступу до всіх ресурсів корпоративної мережі через уніфіковану програму. У цьому випадку форма заяви є додатком до положення про захист інформації, а процедура реєстрації та виконання заявки описана в положенні.

3.3. Захист у хмарі

Хмарне сховище даних - це модель онлайн-сховища, в якій дані зберігаються на численних розподілених в мережі серверах, наданих для користування клієнтами, переважно третьою стороною. На відміну від моделі зберігання даних на власних виділених серверах, придбаних або орендованих спеціально для подібних цілей, кількість або будь-яка внутрішня структура серверів клієнта, загалом,не видна. Дані зберігаються та обробляються у так званій "хмарі", яка є, з точки зору клієнта, одним великим віртуальним сервером. Фізично такі сервери можуть бути розташовані віддалено один від одного географічно.

Рис. 3.1. Схема як працює хмара

Багато великих компаній так чи інакше використовують хмарні технології, найчастіше у формі приватної хмари. Тут важливо пам’ятати, що, як і будь-яка інша техногенна інформаційна система, хмарні служби містять потенційні уразливості, якими можуть користуватися вірусописучі.

Тому, організовуючи доступ навіть до своєї хмари, потрібно пам’ятати про безпеку каналу зв'язку та кінцевих пристроїв, що використовуються з боку співробітників. Не менш важливими є внутрішні політики, які регулюють, яким працівникам доступ до даних у хмарі, або який рівень секретності може зберігатися в хмарі тощо. Компанія повинна мати прозорі правила:

- які служби та сервіси працюватимуть із хмари;
- які служби та сервіси працюватимуть на місцевих ресурсах;
- яку інформацію слід розміщувати в хмарах;
- яку інформацію потрібно тримати «при собі».

3.4. Як організувати багаторівневий захист корпоративних мереж

Ступінь захисту, що вимагається даними корпоративної мережі, безпосередньо визначається їх значенням. Чим більша шкода зазнана власником в результаті втрати інформації, тим повинні бути вжиті більш рішучі заходи. Навіть просто отримавши доступ до Інтернету з персонального комп’ютера, будь-який користувач піддається ризику викрадення його персональних даних зловмисниками. Віруси можна використовувати для копіювання, модифікації або знищення важливих файлів. Щоб захистити себе, досить дотримуватися хоча б найпростіших правил:

1. Продублюйте файли з конфіденційною інформацією на зовнішніх носіях та регулярно їх оновлюйте.

2. Перевірте свій комп’ютер на наявність вірусів за допомогою спеціальних програм. Чим частіше ви це робите, тим краще.

3. Тримайте пристрій підключеним до джерела безперебійного живлення. Так ви встигнете зберегти важливі файли та безпечно вимкнути обладнання у разі раптового відключення електроенергії.

Як показує практика, останнє трапляється найчастіше. Часто трапляються стрибки напруги. Якщо власник комп'ютера не готовий до таких ситуацій, він ризикує втратити не тільки цінні дані, але і сам пристрій: деякі його компоненти можуть вийти з ладу. Придбання ДБЖ (джерело безперебійного живлення) та підключення до нього обладнання не забере у вас багато часу, але гарантовано позбавить вас від можливих неприємностей у майбутньому.

Крім того, питання захисту комп'ютера від вірусів залишається актуальним і сьогодні. Найчастіше користувачі «забирають» їх при відкритті файлів, завантажених з Інтернету. Наприклад, у процесі встановлення неліцензійної програми, знайденої на ненадійному сайті. Віруси також можуть передаватися через месенджери (наприклад, Skype), електронні листи тощо. Щодня база даних про наявні віруси розширюється, зловмисники розробляють нові способи викрадення даних користувачів. Відповідно, антивірусне програмне забезпечення, яке розробляється професіоналами, регулярно вдосконалюється.

Важливо, щоб антивірусні програми купувались безпосередньо у виробників. При цьому їх потрібно постійно оновлювати - причина цього описана вище. Поповнення бази даних відбувається переважно на серверах розробників програмного забезпечення. У більшості випадків одним ПК користується кілька людей, тому необхідно, щоб кожен із них був забезпечений захистом. Для цього ефективно використовуються системні інструменти для створення необмеженої кількості облікових записів на одному пристрої. Для введення кожного з них потрібно підтвердити свою особу, ввівши логін та пароль. Ви також можете зашифрувати дані корпоративної мережі. У цьому випадку отримати доступ до них можна лише за допомогою спеціальних конфіденційних ключів, якими, звичайно, є лише уповноважені особи. Все це актуально для мережевих серверів.

Питання захисту комп’ютера під час перебування у корпоративній мережі слід висвітлювати окремо. Брандмауери призначені для того, щоб впоратися з цим завданням, запобігаючи проникненню різних шкідливих програм з Інтернету. Користувач може визначити критерії, що використовуються для фільтрації даних, отриманих від мережі. Брандмауери допомагають відбивати кібератаки, блокувати підозрілі розсилки тощо. Якщо брандмауер одночасно підключений до кількох корпоративних мереж, він називається брандмауером.

Часто корпоративні дані зчитуються під час їх передачі за каналами зв'язку. Щоб уникнути цього, практикується шифрування інформації корпоративної мережі. Існує навіть наука криптографія, яка вивчає способи її реалізації.

3.5. 9 ефективних засобів захисту корпоративних мереж

1.Засоби захисту інформації від несанкціонованого доступу.

Для запобігання несанкціонованому доступу до системи третіх сторін сьогодні використовуються три типи перевірок: авторизація, ідентифікація, автентифікація.

Суть першої процедури полягає в тому, що користувач повинен увійти в систему, щоб підтвердити, що він має право працювати з даними корпоративної мережі. Він також може використовуватися для диференціації прав доступу працівників до мережевих та комп’ютерних ресурсів.

Ідентифікація - це присвоєння працівникові певного імені, що існує в системі в одному примірнику, та коду (пароля). Останній інакше називається ідентифікатором. І те, і інше необхідно для підтвердження законності своїх дій.

Нарешті, автентифікація - це перевірка даних, які користувач вводить під час входу. Щоб уникнути процедури кожного разу, можна зберегти пароль на ПК, увімкнувши форму.

2. Захист інформації в комп’ютерних мережах.

При підключенні до локальної мережі через Інтернет брандмауери часто відіграють захисну роль. Таким чином, корпоративну мережу можна простою

мовою розділити на дві половини і для кожної з її частин встановити окремі правила. Вони мають на увазі умови, за яких інформація буде проходити через так званий "кордон". Це можна зробити за допомогою як апаратних, так і спеціальних програм.

3. Криптографічний захист інформації.

Шифрування сьогодні дуже успішно використовується для захисту корпоративних даних. Для цього встановлюється певний алгоритм або використовується його реалізуючий пристрій. Тримання процесу під контролем дозволяє мати ключ. Він надає своєму власнику доступ до зашифрованої інформації. В даний час ця техніка вважається однією з найбільш ефективних у галузі захисту. З його розповсюдженням обмін інформацією в Інтернеті або між віддаленими серверами став набагато безпечнішим.

4.Електронний цифровий підпис.

Нерідкі випадки, коли зловмисники перехоплюють надісланий електронний лист і частково виправляють його або замінюють на будь-який шкідливий файл. Щоб уникнути цього, кожному повідомленню присвоюється електронний цифровий підпис. Це той самий лист, але зашифрований приватними ключами. Електронний підпис дозволяє перевірити, чи не змінилось повідомлення, написане воно адресатом чи кимось іншим. При відправленні надсилається некодований лист, але супроводжується підписом. Отримавши повідомлення, одержувач може скористатися відкритим ключем та порівняти між собою вихідний код та підпис. Повна відповідність говорить про цілісність та надійність даних.

5.Захист інформації від комп'ютерних вірусів.

Коли ми говоримо «комп'ютерний вірус», ми маємо на увазі програму, яка може самовідтворюватися та надсилати ці копії на різні носії, замінювати їх файлами та іншими програмами, втручатися в системні процеси тощо. Вони можуть передаватися через канали зв'язку разом з інформацією від користувача до користувача.

Залежно від місцезнаходження всі віруси класифікуються на: Мережеві. Завантажувальний. Програмне забезпечення (їх «жертвами» є файли з роздільною здатністю .com або .exe). Макровіруси. Для боротьби з вірусами використовується спеціальне антивірусне програмне забезпечення. Багато чують назви таких програм, як "Avast", Norton AntiVirus тощо.

6.Брандмауери.

Брандмауери (брандмауери) - це програмне забезпечення чи програмне забезпечення. Їх функція полягає у забезпеченні захисту та контролю волоконних ліній зв'язку, підтримці безпеки корпоративної мережі для підключених до неї користувачів, а також обмеженні доступу до ресурсів системи сторонніх осіб. Ефективність технологій доведена на практиці, тому сьогодні вони активно використовуються у всьому світі.

7.Технологія віртуальних захищених мереж.

Інша його назва - VPN. Цей метод використовується для захисту корпоративної мережі. Технологія дозволяє організувати систему зв'язку таким чином, що неможливо буде незаконно у неї ввійти. Для його створення можна використовувати будь-який тип каналів зв'язку. У цьому випадку повністю виключається можливість перехоплення переданої інформації. Зловмисник не зможе підключитися до системи, якщо він не зареєстрований у ній, отже, він не зможе стерти важливі дані корпоративної мережі, змінити їх, скопіювати, здійснивши кібератаку.

8.Аудит та моніторинг мережі.

Призначення цієї технології - забезпечення безпеки інформаційних ресурсів корпоративної мережі. Це дозволяє відстежувати та контролювати дії, що виконуються користувачами в системі. Таким чином, ви можете своєчасно фіксувати та відображати заплановані атаки ззовні. Крім того, аудит дозволяє перевірити систему захисту на наявність уразливостей.

9.Технологічне рішення BioLink ™.

Технологія BioLink - це вдосконалена процедура ідентифікації. Метод заснований на використанні унікальних біометричних даних користувачів.

Відбитки пальців створюють 500-байтну вибірку, яку хакери неможливо розшифрувати та визначити закодоване зображення. Це виключає можливість маскування сторонніх осіб під зареєстрованими користувачами.

3.6. Як розрахувати прибутковість захисту ресурсів корпоративної мережі підприємства

Визначити фінансову вигоду від використання системи захисту можна таким чином:

(Вдо − Впісля) × Вт = Від, де

Вдо - ймовірність виникнення неприємностей (наприклад, кібератак) до моменту установки захисту

Впісля - той самий показник, але лише після вжиття необхідних заходів.

Вт – втрати

Від - віддача.

Якщо система захисту вимагає більше витрат на свою організацію, ніж отримана віддача, її впровадження для компанії невигідно. З тим самим успіхом можна обійтися звичайною страховкою, і краще звернути увагу на ті аспекти бізнесу, які в даний час є більш важливими. Вони можуть включати, наприклад, роботу електронної пошти. Відповідно до наведеної формули, якщо допустити навіть 1% ймовірність того, що його сервер з якихось причин вийде з ладу через день, продуктивність робочих процесів у компанії зменшиться на 50%.

Розглянемо ситуацію детальніше. Припустимо, що оборот компанії дорівнює 150 мільйонам рублів на рік. Знову ж, скористайтеся формулою і підрахуйте, що у разі припинення електронної пошти компанія зазнає збитків 750 000 грн на рік (150 000 000 * 50% * 1% = 750 000). Однак, якщо є резервні сервери, ймовірність такої ситуації зменшиться до однієї десятої відсотка.

Уявіть, що обслуговування останнього коштує 120 000 грн на рік. Також потрібно платити їх оренду - це 100 000 грн на рік. За таких показників прибутковість становитиме 675 000 грн щорічно.

Оскільки ціна додаткового набору серверів (220 000 грн на рік) не перевищує віддачі, яка складе трохи більше 300%, очевидно, що їх придбання є фінансово виправданим.

Звичайно, не слід сліпо довіряти цифрам. Вони лише допоможуть вам зорієнтуватися в аналізі ситуації на підприємстві. Як підтвердження цьому можна навести ситуацію в компанії, де система активно використовувалася для запобігання вилученню співробітників гнучких дисків та дисків, які могли зберігати важливу інформацію корпоративної мережі. Ідея її впровадження видалася вдалою, за всіма підрахунками, нововведення дало свої результати. Запропоновано цьому працівникові отримати підвищення. Однак ніхто не думав, що проект насправді неефективний: будь-який персонал корпоративних даних може скопіювати та надіслати кудись, не виходячи з офісу (електронною поштою).

3.7. Сучасні технології захисту корпоративних мереж вітчизняних та закордонних розробників

Запобігти потраплянню важливих даних в руки зловмисників можна як за допомогою програмного, так і апаратного забезпечення. Сьогодні захист корпоративних мереж від несанкціонованого вторгнення сторонніми особами можна здійснити величезною кількістю різних способів.

Secret Net

Цей інструмент захисту необхідний для захисту цінної інформації корпоративної мережі від зовнішніх загроз. Secret Net виконує багато функцій, зокрема:

1. Дозволяє автентифікувати користувачів.
2. Контролює канали зв'язку, за якими передаються секретні дані корпоративних мереж, та запобігає їх витоку;
3. Здійснює управління всією системою захисту в цілому, а також при необхідності здійснює її повне сканування.

4. Дозволяє масштабувати покриття системи захисту. Якщо Secret Net доступний в Інтернеті, його можна використовувати навіть у великих компаніях з великою кількістю філій.
5. Створює захищене інформаційне середовище.
6. Виробляє відстеження комп'ютерів та носіїв даних, зареєстрованих у системі.

ViPNet Custom

ViPNet Custom - це набір спеціальних технологій для захисту секретної інформації, зокрема персональних даних. Ефективність методики дозволяє використовувати її навіть у великомасштабних системах зв'язку, таких як різні сервери, робочі станції тощо. ViPNet Custom вирішує зразу дві важливі завдання:

Забезпечення умов для безпечної передачі важливої інформації. Для цього використовуються різні канали зв'язку VPN (наприклад, Інтернет, бездротові лінії, телефони). Керують ними уповноважені особи із спеціальних центрів.

Створення центру сертифікації з метою надання замовнику можливості використовувати електронні цифрові підписи та сертифікати у своїй діяльності. Вони використовуються в банківських системах, оформленні документів, при роботі з електронною поштою та ін. Важливо мати можливість взаємодіяти з продуктами PKI інших російських компаній.

CryptoPro

CryptoPro - це програма, яка дозволяє захищати цінні корпоративні дані за допомогою електронних цифрових підписів та шифрування. Не має значення, де подається інформація: чи це базове офісне програмне забезпечення, чи складні спеціалізовані програми для документації.

Антивірусне програмне забезпечення

Більшість існуючих на сьогодні антивірусів розроблено для різних версій Windows. Перш за все, це пояснюється, звичайно, тим, що ця ОС встановлена на більшості комп’ютерів, тому кількість вірусів, створених для її атаки, перевищує кількість інших шкідливих програм.

Брандмауер

Брандмауер став стандартною технологією в галузі захисту корпоративних мереж від незаконного вторгнення. Він має кілька різновидів, найпоширенішими з яких є: Fortigate 60C - по суті це програмний та апаратний брандмауер, але дещо вдосконалений і має ширший спектр функцій, ніж стандартна версія; UserGate 5.2F (може використовуватися як суто програмне та інтегроване програмне та апаратне забезпечення); ME ViPNet комплекс; Технологія SSEP - персональний брандмауер, що дозволяє відображати вірусні атаки, відстежувати витік даних у корпоративних мережах та спроби несанкціонованого впровадження.

Висновки до третього розділу

1. Розроблені практичні поради щодо поліпшення захисту.
2. Розроблені поради щодо розробки нормативних документів.
3. Розроблено 9 ефективних засобів захисту корпоративних мереж .
4. Досліджено сучасні технології захисту корпоративних мереж вітчизняних та закордонних розробників

ВИСНОВКИ

В роботі проведено дослідження та аналіз існуючих загроз захисту корпоративної мережі хостингової компанії.

Досліджені існуючі проблеми захисту корпоративних мереж хостингових компаній. Визначено методи та засоби захисту корпоративних мереж хостингових компаній.

Розроблені практичні поради щодо поліпшення захисту, щодо розробки нормативних документів.

Досліджено сучасні технології захисту корпоративних мереж вітчизняних та закордонних розробників

У роботі запропоновані ефективні засоби захисту корпоративних мереж.

Таким чином, правильна реалізація вищевказаних та розроблених методів захисту має забезпечити ефективний захист корпоративної мережі хостингової компанії.

ПЕРЕЛІК ПОСИЛАНЬ

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. 4-е изд. / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2012. – 943 с.

2. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;

3. Скиба В.Ю. Руководство по защите внутренних угроз информационной безопасности / В.А. Курбатов. – Спб.: Питер, 2008. – 320 с.

4. Касперски К. Техника сетевых атак / К. Касперски – М.: СОЛОН-Р, 2001. – 304 с.

5. Юдін, О.К. Інформаційна безпека держави / О. К. Юдін, В. М. Богуш. — Харків: Консум, 2004. — 508 с.

6. Крижанівський, О. Положення про конфіденційну інформацію (комерційну таємницю) – базовий документ економічної безпеки фірми // О. Крижанівський // Інтелектуальна власність. – 2006. – № 3. – С. 33-35.

7. Процедура разработки систем программно-технической защиты программного обеспечения [Електронний ресурс] / Середа С. А. – Режим доступу: https://web.archive.org/web/20070913085828/http://consumer.stormway.ru/prottech.htm

8. Корпоративна мережа [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Корпоративна_мережа

9. Хостинговая компанія [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Хостингова_компанія

10. Забезпечення безпеки корпоративної мережі [Електронний ресурс] – Режим доступу: http://www.telesphera.net/blog/network-security.html

11. Биячуев Т.А. / под ред. Л.Г.Осовецкого. Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.

12. Соколов А.В., Шаньгин В.Ф. Защита информации в распределённых корпоративных сетях и системах, - М.:ДМК Пресс, 2002. – 626с.

13. С. Браун. Виртуальные частные сети.. – Лори, 2001– 503 с.

14. С. В. Запечников, Н. Г. Милославская, А. И. Толстой. Основы построения виртуальных частных сетей. Для высших учебных заведений. СПб.: Питер, 2003. – 248 с.

15. Кулаков Ю.А., Луцкий Г.М. Локальные сети, - К.: Юниор, 2008. – 336с.

16. Компьютерные сети. Принципы, технологии, протоколы/ В.Г.Олифер, Н.А.Олифер. – СПб.: Питер, 2001. – 672с.

Демонстраційні матеріали