УДК 004.94 DOI: 10.31673/2412-4338.2019.020513

Шушура О.М., Довбешко С.В., Золотухіна О.А., Асєєва Л.А.
Державний університет телекомунікацій, Київ

ФАКТОРИ СТВОРЕННЯ СТРАТЕГІЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ СУЧАСНОГО ПІДПРИЄМСТВА

В роботі проведено аналіз стану інформаційної безпеки сучасного підприємства та розглянуті проблеми, що виникають у роботі інформаційних систем. Надано рекомендації фахівцям підрозділів інформаційних технологій щодо побудови стратегії інформаційної безпеки. Структуровані процеси інформаційної безпеки для постачальників продуктів і послуг, сформовано підходи до побудови архітектури системи захисту інформаційних мереж, стійкої до загроз. Розглянуто кроки до прискорення реакції на загрози, залучення для підвищення рівня кібербезпеки штучного інтелекту та хмарних технологій.

Ключові слова: *інформаційна безпека, інформаційна система підприємства, загрози*

Shushura O.M., Dovbeshko S.V., Zolotukhina O.A., Asieieva L.A.
State University of Telecommunications, Kyiv

FACTORS FOR CREATING A SECURITY STRATEGY FOR INFORMATION TECHNOLOGIES OF MODERN ENTERPRISE

The purpose of this work is to analyze the current state of information security of modern enterprises and to provide recommendations for the construction of a protection strategy for information technology. In order to achieve this goal, the state of information security of the enterprise is analyzed, problems that arise in the work of information systems are considered, and recommendations are given to specialists of information technology units regarding their solution.

The problem of increasing the threat of cyber espionage and sabotage for enterprises on the example of energy industry organizations is considered and the necessity of understanding by the heads of information technology departments of risks of information security and objects of protection is stated. A set of recommendations is proposed to increase funding for information security measures that can be used by cyber security officials. The disappearance of the perimeter of the information network is considered in detail as one of the main modern factors of the cybersecurity strategy. The use of artificial intelligence technology can simplify initial analysis of network activity, filter out what is normal, and focus efforts on investigating and eliminating high-risk threats. One of the important areas for improving information security is the certification of business websites for online trust audits. The introduction of advanced 5G technologies and the use of IoT services in the work of telecommunications companies increases the threats to information systems. It is recommended to use closed loop automation (CLA), which uses machine learning and artificial intelligence, to evaluate the state of the network in real time. Attention is paid to the analysis of the organization of work with the personnel of the enterprise as the main factor of reliability of the information security system, the basic rules of cyber hygiene are given.

The results of the work can be used to develop a strategy for information security of enterprises, including telecommunication companies using modern 5G technologies and IoT services in their work.

Keywords*: information security, enterprise information system, threats*

Шушура А.Н., Довбешко С.В., Золотухина О.А., Асеева Л.А.
Государственный университет телекоммуникаций, Киев

ФАКТОРЫ СОЗДАНИЯ СТРАТЕГИИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ СОВРЕМЕННОГО ПРЕДПРИЯТИЯ

В работе проведен анализ состояния информационной безопасности современного предприятия и рассмотрены проблемы, возникающие в работе информационных систем. Даны рекомендации

специалистам подразделений информационных технологий по построению стратегии информационной безопасности. Структурированы процессы информационной безопасности для поставщиков продуктов и услуг, сформированы подходы к построению архитектуры системы защиты информационных сетей, устойчивой к угрозам. Рассмотрены шаги к ускорению реакции на угрозы, привлечения для повышения уровня кибербезопасности искусственного интеллекта и облачных технологий.

***Ключевые слова**: информационная безопасность, информационная система предприятия, угрозы*

Вступ

Число кібератак на об'єкти критичної інфраструктури зростає з кожним днем в геометричній прогресії. З'являються ряд критичних точок відмови, при цьому будь-яке порушення в ланцюжку поставок може призвести до тяжких наслідків. Підключення інформаційних систем управління підприємством до Інтернету розширюється. Значна кількість інформаційних систем підприємств критичної інфраструктури, що використовуються сьогодні, було розроблено і впроваджено до того, як безперервне підключення до Інтернету стало нормою. Багато компонентів промислових систем мають вбудовані можливості віддаленого управління, але в них частково або повністю відсутні протоколи безпеки. Більш того, у деяких системах ніколи не було вбудованих засобів контролю інформаційної безпеки, які ми вважаємо цілком очевидним сьогодні. Перехід цих систем в Інтернет відкрив їх для безлічі атак.

Основна частина

Метою даної роботи є аналіз сучасного стану інформаційної безпеки сучасних підприємств і надання рекомендацій щодо побудови стратегії захисту інформаційних технологій. Для досягнення поставленої мети в роботі проаналізований стан інформаційної безпеки підприємства, розглянуті проблеми, що виникають у роботі інформаційних систем та надаються рекомендації фахівцям підрозділів інформаційних технологій щодо їх вирішення.

1. Кібершпіонаж і диверсії створюють все більшу загрозу для підприємств

Критична інфраструктура за своєю природою є цікавою метою для іноземної держави, навіть у мирний час. Наприклад, взаємопов'язаність об'єктів в енергетичній галузі підсилює вразливість системи, і кібератаки часто залишаються непоміченими протягом деякого часу. Вважається, що мережа електростанцій і ліній, що з'єднують будинки і підприємства, є однією з найбільш важливих інфраструктур в світі. Це також один з об'єктів, які найбільш часто піддаються нападам, з наслідками, що можуть потенційно вийти далеко за межі енергетичного сектора.

Звіт фінської компанії F-Secure [1] показує, що:

- різноманітні противники, кожен зі своєю мотивацією, постійно прагнуть скомпрометувати організації, які експлуатують критично важливу інфраструктуру;
- зловмисники мають більше часу, ніж їхні цілі, і на планування їх атаки йдуть місяці;
- люди є найслабшою ланкою у виробництві, а співробітники компанії, мабуть, стають метою злочинців;
- зловмисники продовжують домагатися успіху головним чином через відсутність в організаціях зрілих практик інформаційної безпеки;
- певні групи IT-фахівців продовжують шукати уразливі місця і шпигунські можливості, переслідуючи політичні цілі;
- існує безліч шкідливих програм / методів, націлених на енергетичну галузь, причому фішинг є найбільш поширеним методом початкової атаки ланцюжка поставок;
- утримати невелику поверхню атаки в енергетичній галузі просто неможливо.

Незважаючи на те, що порушення неминучі, організаціям для підтримки ефективності бізнесу необхідно переглянути свій стан інформаційної безпеки для впровадження новітніх

технологій, таких як рішення для виявлення і реагування на складні загрози і цільові атаки (endpoint detection and response - EDR).

У новому звіті Deloitte Global «Управління кіберризиками в електроенергетичному секторі» [2] оцінюються найбільші кіберзагрози в електроенергетичному секторі та вказується, як компанії можуть управляти цими ризиками.

Сектор електроенергетики стикається з швидко зростаючим ландшафтом кіберзагроз – витонченість, частота атак, а також число учасників загроз зростає. Фактично, енергетика є одним з провідних секторів, на які націлені кібератаки. Загрози можуть варіюватися від внутрішніх, таких як атака незадоволених співробітників, до зовнішніх, від урядів ряду держав або організованої злочинності.

Електроенергетичні компанії повинні зробити ряд кроків для подолання цих перешкод і управління кіберризиками на підприємстві:

1. Скласти карту активів інфраструктури та оцінити вразливості. Електроенергетичні компанії повинні зіставити активи інфраструктури і розставити пріоритети по їх важливості. Потім вони повинні визначити вразливості активів і оцінити зрілість контрольного середовища для управління загрозами. І, нарешті, компанії повинні створити основу для захисту критично важливих активів з використанням людей, процесів і технологій.

2. Оцінити процеси забезпечення безпеки постачальників. Для управління кіберризиками в ланцюжку поставок багатообіцяючим першим кроком є участь у функції закупівель в ланцюжку поставок. Електроенергетичні компанії повинні розуміти процеси кібербезпеки постачальників для продуктів і послуг і забезпечувати їх відповідність провідним галузевим практикам. Безсумнівно підвищують прозорість поставок довірчі принципи, закладені в практиках блокчейна.

3. Співпрацювати з колегами по галузі і державними установами. Управління ризиками кібербезпеки не повинно припинятися на рівні окремих підприємств. Енергетичні компанії можуть поліпшити стан кібербезпеки, допомагаючи встановити галузеві стандарти, обмінюючись інформацією щодо загроз зі колегами і впроваджуючи нові технології. Зростаюча складність технологічного середовища є дуже важливим фактором для обміну інформацією про загрози.

4. Датчики і системи безпеки повинні обмінюватися інформацією про загрози в реальному часі, щоб відповідати швидкості атаки. Технологічні інновації та аналітика повинні визначати стратегію кібербезпеки кожної електроенергетичної компанії. Нові інструменти стають все більш доступними, і можливості для моніторингу мереж в режимі реального часу, виявлення загроз і їх усунення швидко розвиваються, забезпечуючи необхідний захист для галузі в цілому.

Керівники підрозділів IT-безпеки (Chief Information Security Officer - CISO), що працюють в енергетичних і промислових організаціях, повинні розуміти ризики кібербезпеки, з якими вони стикаються, і точно визначати, що потрібно захищати.

Експерти, що володіють найкращими знаннями про завод і його системи, можуть дати оцінку, щоб допомогти новим CISO скласти уявлення про те, які у них уразливості і наскільки вони серйозні [3]. CISO повинні інформувати себе і свої команди про стандарти кібербезпеки для бізнесу, а потім впроваджувати і завжди дотримуватися цих стандартів. Наприклад, їм слід ознайомитися з ISA99 / IEC 62443, суворим стандартом для технологій промислової автоматизації [4].

2. Необхідне фінансування - основа забезпечення інформаційної безпеки

Збільшити фінансування для забезпечення інформаційної безпеки - непросте завдання, особливо коли організація стикається з бюджетними обмеженнями.

Тому для отримання достатнього фінансування необхідно:

1. Визначити цінні активи підприємства та ризики, викликані організаційними недоліками. Слід описати найбільш важливі активи компанії і спрогнозувати, як атака на комп'ютерні системи може негативно вплинути на прибутковість та імідж бізнесу.

2. Розставити пріоритети і оцінити поточні ризики організації. Визначити п'ять основних ризиків інформаційної безпеки компанії - ті, які мають найбільший потенційний вплив на організацію - і оцініть сильні і слабкі сторони підприємства, а також прийнятні рівні ризику з точки зору людей, інформації, процесів, програм та інфраструктури.

3. Розробити план управління ризиками з точки зору:

• управління інформаційними активами;

• підвищення рівня безпеки;

• підвищення стійкості мережі.

4. Описати план безпеки для врахування поточних рівнів ризику:

• існуючі елементи управління, такі як покупка і впровадження послуг, ліцензії, розробка конфігурації, підтримка і таке інше;

• внутрішнє, зовнішнє або комбіноване рішення для захисту даних, щоб розширити можливості виявлення і зменшити ймовірність злому конфіденційної інформації і знизити ризик від критичного до низького;

• пропоновані контрольні ресурси до кожного кварталу.

Необхідно показати, чому запропонована стратегія інформаційної безпеки буде успішною, уточнити позитивні очікування після впровадження стратегії, встановити контрольні показники успіху і прогресу для програми врядування та інвестицій.

3. Зникнення периметру інформаційної мережі як фактор стратегії кібербезпеки

Концепція інформаційної мережі підприємства, повністю закритої всередині будівлі або віртуальної організації і, отже, більш зручною для захисту, фактично зникла. Це не новина для тих, хто в змозі захистити організацію від кібератак, і можна зрозуміти проблеми, з якими команди безпеки стикаються в цих обставинах.

Зникнення периметра викликає розширення мережі організації, що включає в себе набагато більше пристроїв і місць розташування, багато з яких знаходяться за межами того, що раніше вважалося периметром. Багато пристроїв і таких місць знаходяться поза контролем команди безпеки. Gartner прогнозує [5], що до 2021 року 27 відсотків корпоративного трафіку даних обійдуть захист периметра і будуть безпосередньо передаватися з мобільних і переносних пристроїв в хмару. Очікується, що число пристроїв IoT, які, як відомо, є слабкими з точки зору безпеки та вразливості, збільшиться майже втричі в наступні 6 років з 26,7 млрд. у 2019 до 75,4 млрд. у 2025 році. За даними LogicMonitor [5], до 2020 року 83% корпоративних робочих навантажень будуть знаходитися в хмарі. Хмара вимагає нових тактик безпеки для вирішення проблеми природи хмари як середовища, безпеку, яка не забезпечується ні хмарними провайдерами, ні локальними інструментами безпеки.

Коли відділам інформаційних технологій підприємств потрібно тільки патрулювати периметр, обсяг вхідних і вихідних дій був керованим. Тепер обсяг даних, що генеруються, на кілька порядків перевищує можливості груп безпеки з контролю за всім цим. Ця розширена поверхня атаки включає IoT, персональні пристрої і хмару. Захист периметру легко обійти за допомогою розширених загроз, які ухиляються від виявлення.

Існує кілька методів і технологій, які дозволять групам безпеки ефективно захищати свою мережу, як тільки вони прийдуть до згоди з тим фактом, що периметр легко обходиться. Всі вони пов'язані з тими засобами, що зосереджені на виявленні зловмисного бокового руху в мережі, що є найбільш важливою метою для організацій сьогодні. Брандмауери, захист кінцевих точок і інші засоби захисту периметра важливі, але їх недостатньо.

В першу чергу слід забезпечити безпечне спілкування. Кожен вузол - це будь-який комп'ютер, пристрій або система, підключена до хмари або мережі, наприклад, ноутбук, смартфон і принтер із загальним доступом. Слід контролювати і аналізувати зв'язок між цими пристроями на предмет чого-небудь незвичайного або шкідливого. Якщо злочинець може зламати iPad, він може перейти звідти до інших пристроїв у середовищі підприємства, до інших вузлів мережі. З огляду на інтенсивність активності серед всіх вузлів зростаючої

мережі, командам по забезпеченню безпеки може бути складно стежити за всіма оповіщенням. Один з варіантів - просто найняти більше аналітиків, але при нестачі навичок це теж може виявитися складним завданням. Деякі інструменти мережевої аналітики дозволяють користувачам встановлювати поріг для того, що буде генерувати попередження. Підвищення порогу зменшить кількість попереджень, але підвищить ризик пропуску атаки.

Інший варіант - використовувати штучний інтелект (ШІ). Рішення для забезпечення безпеки на базі ШІ може створювати моделі нормальної активності і автоматично виділяти те, що є незвичайним або аномальним, що може вказувати на зловмисну діяльність.

Знання того, що щось передається між двома пристроями або вузлами, недостатньо. Необхідно проаналізувати характер спілкування. Знання того, що деякі рухи є аномальними або незвичайними в порівнянні з встановленими базовими рівнями, корисно. Це перший крок у виявленні загроз, що діють у мережі підприємства. Але є недолік у використанні тільки виявлення аномалій: не всі аномалії є шкідливими. Включення даних про відомі зловмисні дії в раніше згаданий аналіз на основі ШІ може відокремити шкідливі аномалії від доброякісних, майже виключити помилкові спрацьовування і зосередити зусилля груп безпеки на бічному русі, що представляє найбільший потенційний ризик.

Для захисту мережі тепер потрібні моніторинг і аналіз бокового руху в розширеній мережі. Це оптимально досягається за допомогою ШІ, який може спростити початковий аналіз мережевої активності, відфільтрувати те, що є нормальним, та зосередити зусилля на розслідуванні та усуненні загроз високого ризику.

4. Сертифікація сайтів підприємств для онлайн-аудиту довіри

Від глобальної економіки до щоденних індивідуальних взаємодій, все більше і більше часу люди проводять в Інтернеті. Проте, рівень уваги до захисту даних і захисту конфіденційності дій споживачів продукції підприємств є поки що недостатнім.

Біля 70 відсотків веб-сайтів США були сертифіковані для онлайн-аудиту довіри і рейтингу добробуту у 2019 році, що є найвищим показником за всю історію, в порівнянні з 52 відсотками в 2017 році, головним чином завдяки покращенням у аутентифікації електронної пошти та шифруванні сеансів [6].

В цілому, аудит виявив сильний крок в сторону шифрування: 93 відсотки сайтів шифрують всі веб-сеанси (в порівнянні з 52 відсотками у 2017 році). Аутентифікація електронної пошти також знаходиться на рекордно високому рівні; 76 відсотків сайтів використовують і SPF, і DKIM (проти 48 відсотків у 2017 році), а 50 відсотків мають запис DMARC (проти 34 відсотків раніше). Однією з можливостей покращання в цьому напрямі є використання механізмів звітності про вразливість, які різко зросли в онлайн-рітейлі, новинних і хостингових компаніях, але в цілому використовувалися тільки 11 відсотками організацій. Альянс онлайн-довіри домігся значних успіхів у просуванні більш високих стандартів безпеки в Інтернеті [6].

5. Автоматизація із замкнутим контуром для боротьби із загрозами безпеці IoT в епоху 5G

Впровадження 5G потенційно може привести до появи додаткових векторів загроз в мережах операторів, тому постачальники комунікаційних послуг (Communication Service Providers - CSPs) мають вирішити проблеми безпеки IoT, і, згідно з недавнім звітом Allot Telecom Trends [8], автоматизація з використанням замкнутого циклу (Closed Loop Automation - CLA) може допомогти їм вирішити цю проблему.

Автоматизація із замкнутим контуром (CLA), яка використовує машинне навчання і штучний інтелект, пропонує безперервну оцінку стану мережі в реальному часі, доступності ресурсів і вимог до трафіку для виявлення перевантажень мережі, шкідливого трафіку на основі IoT. CLA допомагає виявляти та ізолювати нові аномалії і пом'якшувати загрози, перш ніж вони зможуть впливати на інформаційну мережу. Ця технологія одночасно допомагає підвищити продуктивність і забезпечує аналіз ємності, контроль якості і виявлення помилок.

Хоча цінність CLA очевидна, і багато CSPs бачать переваги застосування CLA, оскільки 5G стає реальністю, багато підприємств поки не використовують його в повній мірі. Деякі загальні перешкоди для прийняття CLA включають в себе проблеми з набором навичок, проблеми з витратами і низьке розуміння технологій. У згаданому вище звіті Telco Trends від Allot вказується, що 25% CSPs не мають необхідних навичок, 22% не розбираються в технологіях, а 20% стурбовані витратами.

Необхідно акцентувати, що для тих CSPs, які хочуть ідентифікувати свій бренд за допомогою безпеки, існує безпрецедентний ресурс з інструментами CLA і керівництвом по боротьбі із загрозами безпеці IoT. CSP звертаються до незалежних постачальників послуг (independent service vendors - ISV) за інструментами CLA. Незалежні розробники ПЗ використовують ШІ для створення навчального програмного забезпечення, яке автоматично виявляє нові проблеми і миттєво вирішує їх, ґрунтуючись на вивчених шаблонах і прикладних моделях, які негайно адаптуються до нових даних.

6. Основа інформаційної безпеки підприємства – його співробітники.

Інформація безпека підприємства залежить в першу чергу від поведінки його співробітників [8]. Звинувачувати працівників в поведінці, до якої вони звикли в особистому житті, складно. Це може додати додаткову складність для IT-фахівців із захисту активів компанії, оскільки необхідно враховувати повсякденні звички співробітників, що може поставити під загрозу безпеку організації.

По-перше, співробітники мають потребу в навчанні. Тому ті, хто регулярно використовує загальнодоступні Wi-Fi, Bluetooth або USB-накопичувачі в особистому житті, повинні розуміти, чому вони небезпечні для роботи.

Потім організація повинна розвивати культуру спілкування - наприклад, якщо щось йде не так, співробітники також повинні відчувати себе досить комфортно, щоб повідомляти про проблеми в IT, перш ніж буде завдано значної шкоди.

Співробітники повинні знати, що якщо вони втратять смартфон або ноутбук, вони повинні негайно повідомити про це IT. При проведенні тренінгів з безпеки навчальна програма повинна включати подробиці і контекст того, як повідомлення про втрачений або вкрадений пристрої відразу ж дозволяє IT-відділу заблокувати його до того, як інформація може бути вкрадена. Менеджери мають цінувати чесність - краще отримати помилкову тривогу, чим ризикувати скомпрометувати пристрій.

Співробітники повинні знати проблеми з Wi-Fi і Bluetooth. Співробітники, яким доводиться платити за тарифні плани, звикли шукати відкриті з'єднання Wi-Fi всюди, де б вони не знаходилися. Звичайно, вони чули, що загальнодоступний Wi-Fi небезпечний, але якщо з ними нічого поганого не станеться під час його використання, вони часто проігнорують попередження. Важливо пояснити, як з'єднання Wi-Fi дозволяє хакеру легко розташуватися між пристроєм співробітника і точкою доступу, отримуючи доступ до кожної частини інформації, яку вони відправляють через Інтернет, включаючи всю їхню особисту інформацію, а також облікові дані для безпеки мережі бізнесу. Є навіть онлайн-уроки з мільйонами переглядів, щоб показати хакерам, як це зробити. Отримавши інформацію про співробітника - ділову або особисту - кіберзлочинці можуть легко увійти в систему і видати себе за них у будь-який час. Через загальнодоступний Wi-Fi хакери можуть також відправляти спливаючі повідомлення, що пропонують оновлення програмного забезпечення, де при натисканні вони встановлюють шкідливе ПЗ і заражають пристрій.

Використання Bluetooth також небезпечно. Восени минулого року злодії скористалися недоліками безпеки для злому з'єднань і крадіжки бізнес-даних з корпоративних мереж. Як тільки пристрій заражено, він легко поширює шкідливе ПЗ на інші прилеглі пристрої, включаючи офісні комп'ютери. Хоча більшість пристроїв були виправлені для цієї конкретної проблеми, хакери, як правило, на крок попереду виробників пристроїв, а це може означати, що в майбутньому можуть виникнути інші неприємні сюрпризи.

Щоб уникнути проблем безпеки, пов'язаних з Wi-Fi, Bluetooth і іншими небезпечними сполуками, співробітникам підприємства слід використовувати віртуальну приватну мережу (VPN). VPN - це приватний зв'язок, яке шифрує весь трафік, захищаючи дані компанії.

Однак мережі VPN складно налаштувати, і використання неправильного протоколу може привести до недоліків безпеки. Одне дослідження показало, що 38 відсотків безкоштовних Android VPN доступні з шкідливим ПЗ.

Окремо слід відмітити небезпеку USB-накопичувачів. Переважна більшість доступних даних на них не зашифровано, що дозволяє хакерам перепрограмувати їх за допомогою шкідливих програм. Оскільки вони такі маленькі, флешки також легко втратити. Недавнє дослідження показало, що з 90 відсотків співробітників, які використовують USB-накопичувачі, 80 відсотків з них не використовують зашифровані USB-накопичувачі. Що ще гірше, те ж саме дослідження показало, що 87 відсотків опитаних співробітників зізналися, що втратили флеш-накопичувач, який використовується для роботи, і не повідомляли про це.

Незахищені уразливості, а також зростаюча складність мереж і додатків підприємства створюють постійний ризик для його інформаційної безпеки.

Аналізуючи найбільші результати в області безпеки за останній рік, Keysight випустила третій щорічний звіт з безпеки від дослідницького центру Ixia [9] з аналізу додатків і загроз (ATI).

У 2018 році Ixia виявила 662 618 фішингових сторінок і 8 546 295 сторінок, розміщених або заражених шкідливими програмами, тому для успішної атаки потрібно всього один хибний клік по електронній пошті або посиланням. Ретельно продуманий і своєчасний фішинг може спонукати навіть досвідчених користувачів натискати на скомпрометовані посилання. Успішний захист залежить від комбінації проактивного навчання користувачів, блокування фішингових атак і шкідливих програм, які перетинають кордон мережі, а також виявлення та блокування бічного руху в мережі.

Крипто-джекінг продовжує зростати. Ця загроза досягла нового піку в 2018 році, коли хакери об'єднали кілька класичних атак для доставки майже автономного шкідливого ПЗ.

IT-постачальники створили код або конфігурації, які призвели до численних успішних порушень безпеки в 2018 році, але відповідальність за це також розділили IT-фахівці та співробітники служби безпеки. Відомі атаки і вектори атак залишалися успішними, тому що співробітники служби безпеки не усували уразливості і не встановлювали виправлення.

Навчання співробітників відповідального використання своїх пристроїв і повідомленням про втрату або крадіжку є важливою частиною процесів інформаційної безпеки підприємства.

Основні правила кібергігієни сформульовані у джерелі [10]:

1. Використовуйте ліцензійні/легалізовані операційні системи, інші програмні продукти, своєчасно і систематично їх оновлюючи.

2. Користуйтеся антивірусним програмним забезпеченням з технологією евристичного аналізу.

3. Використовуйте програмний міжмережевий екран (брандмауер) і штатні засоби захисту від шкідливого програмного забезпечення.

4. Робіть регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SDD, HDD і т.д.) і налаштуйте функцію «відновлення системи».

5. Не підключайте флешки і зовнішні диски, не вставляйте CD і DVD і т.д. в ваш комп'ютер, якщо ви не довіряєте повністю їх джерелам. Існують техніки злому комп'ютера ще до того, як ви відкриєте файл на флешці і задовго до того, як ваш антивірус його просканує. Якщо ви знайшли пристрій всередині офісу або на вулиці, отримали його поштою або з доставкою, або незнайомець дав вам його з проханням роздрукувати документ, або просто відкрити і перевірити його вміст - є велика ймовірність, що пристрій є небезпечним.

Довіряйте тільки власним пристроям і будьте обережні з пристроями, які отримуєте від інших людей по роботі або в інших цілях. При підключенні пристроїв забезпечте їх автоматичну перевірку на наявність шкідливого програмного забезпечення.

Вимикайте автоматичний запуск змінних носіїв інформації (захист від autorun.inf).

6. Не зберігайте дані аутентифікації в легкодоступних місцях (наприклад, на робочому столі). Використовуйте для зберігання паролів спеціальні програмні засоби (наприклад, KeePass). створюйте стійкі паролі та не дублюйте їх в інших акантах.

7. Уникайте використання Інтернет-банкінгу, електронних платіжних систем, введення аутентифікації даних при доступі до Інтернету через загальнодоступні (незахищені) бездротової мережі (в кафе, барах, аеропортах та інших громадських місцях).

8. Будьте особливо обережними з відкриттям вкладень до електронної пошти від невідомих осіб. Сьогодні найактуальнішим засобом розсилки шкідливого програмного забезпечення є електронна пошта. Під час роботи з поштою потрібно перевіряти розширення вкладених файлів і не відкривати файли навіть з безпечними розширеннями. Не переходьте з невідомих посиланнях і не завантажуйте файли, які мають потенційно небезпечне розширення (наприклад: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js і т.д.) і навіть безпечне (наприклад: .docx, .zip, .pdf), адже можуть використовуватися уразливості, макроси і інші небезпеки. Звертайте увагу на ім'я електронної пошти: навіть якщо воно здається легітимним, все одно потрібно перевірити (в телефонному режимі або будь-яким іншим способом), чи дійсно ця особа відправляло вам повідомлення з вкладенням.

Іноді буває важко відрізнити шкідливі файли від легітимних. Користуйтеся сервісом VirusTotal для перевірки підозрілих файлів шляхом їх одночасного сканування більше 50 антивірусами. Це набагато ефективніше, ніж сканування файлів антивірусом в автономному режимі, але враховуйте той факт, що завантажуючи файли на VirusTotal, ви надаєте доступ до нього третій стороні. Звертаємо вашу увагу на те, що, навіть якщо перевірка на VirusTotal не дала результату, це не виключає того, що файл може бути шкідливим.

9. При користуванні Інтернет-ресурсами (Інтернет-банкінгом, соціальними мережами, системами обміну повідомленнями, новинами, онлайн-іграми) не знімайте підозрілі посилання (URL), особливо ті, що вказують на сайти, які ви зазвичай не відвідуєте. Будьте уважним до проявів Інтернет-шахрайства. Найпоширенішим засобом введення в оману в мережі Інтернет є фішинг. Особливу увагу слід звертати на доменне ім'я Інтернет-ресурсу, який запитує дані аутентифікації, перш ніж натиснути на посилання: зловмисники можуть замаскувати доменне ім'я, щоб воно виглядало знайомим (facelook.com, goooogle.com т.д.). В іншому випадку велика ймовірність потрапити на фішинг і самостійно «віддати» власні аутентифікаційні дані.

У разі необхідності введення аутентифікації даних переконайтеся в тому, що використовується захищене з'єднання HTTPS, перевіряйте SSL-сертифікат сайту, щоб переконатися, що він не клонований або не підроблений.

Шкідливі URL-адреси можуть бути закодовані у вигляді QR-кодів і / або роздруковані на папері, в тому числі у формі скорочених URL, згенерованих спеціальними сервісами на зразок tinyurl.com, bit.ly, ow.ly тощо. Не вводьте ці посилання в браузер і не скануйте QR-коди вашим смартфоном, якщо ви не впевнені в їх походженні.

Використовуйте VirusTotal для перевірки підозрілих посилань так само, як для сканування файлів.

10. Будьте обережні щодо спливаючих вікон і повідомлень в вашому браузері, програмах, операційній системі і мобільному пристрої. Завжди читайте зміст цих вікон і не натискайте клавіш похапцем.

11. При використанні віддаленого доступу необхідно обмежити доступ за допомогою «білого списку» (IP whitelisting).

12. Встановіть обмеження кількості введення помилкових логінів / паролів. Регулярно переглядайте журнали логування, планувальник завдань і автозавантаження на предмет несанкціонованих дій. Слідкуйте за новинами про нові кіберзагрози і швидко реагуйте на нові виклики.

Висновки. В роботі проведено аналіз стану інформаційної безпеки сучасного підприємства та розглянуті фактори, які на неї впливають. По кожному напрямку

забезпечення інформаційної безпеки надано рекомендації фахівцям відділу інформаційних технологій. Розглянуто кроки до прискорення реакції на загрози, залучення для підвищення рівня кібербезпеки штучного інтелекту та хмарних технологій. Результати роботи можуть бути застосовані для розробки стратегії інформаційної безпеки підприємств, в тому числі телекомунікаційних компаній, що використовують у своїй роботі сучасні технології 5G та сервіси IoT.

References

1. Cyber espionage and sabotage attacks pose an increasing threat to the energy industry. *Help Net Security* (2019), April 17.

2. Evaluating the biggest cyber threats to the electric power sector. *Help Net Security* (2019), February 4.

3. Zeljka Zorz, Building a sound security strategy for an energy sector company. *Help Net Security* (2018), July 30.

4. Which organizations place a premium on security and privacy? *Help Net Security* (2019), April 18.

5. John DiLullo, The perimeter is vanishing, how will you secure your network? *Help Net Security* (2019), April 18.

6. One hundred percent of endpoint security tools eventually fail. *Help Net Security* (2019), April 18.

7. Robert MacDonald, Employee cybersecurity essentials part 2: Lost devices and unsafe connections. *Help Net Security* (2019), April 16.

8. Arthur Zavalkovsky. Closed loop automation combats IoT security threats in the 5G age. *Help Net Security* (2019), April 10.

9. Bad security hygiene still a major risk for enterprise IT networks. *Help Net Security* (2019), April 16.

10. Basic rules of cyber hygiene, April 20 (2019). https://cert.gov.ua/recommendations/21.

Автори статті (Authors of the article)

Шушура Олексій Миколайович – д.т.н., доцент, завідувач кафедри системного аналізу (Shushura Oleksii Mykolaiovych – Doctor of Technical Sciences, Associate Professor, Head of the Department of System Analysis) Phone:+380 (50) 470 15 67. E-mail: leshu@i.ua.

Довбешко Станіслав Володимирович – к.т.н, доцент, директор Навчально-наукового інституту захисту інформації (Dovbeshko Stanislav Volodymyrovych – PhD in Technics, Associate Professor, Director of the Educational-scientific Institute of Information Security). Phone:+380 (67) 503 47 33. E-mail: bezpeka_tzi@ukr.net.

Золотухіна Оксана Анатоліївна – к.т.н., доцент кафедри системного аналізу (Zolotukhina Oksana Anatoliivna – PhD in Technics, Associate Professor of the System Analysis Department). Phone:+380 (95) 510 12 40. E-mail: zolotukhina.oks.a@gmail.com

Асєєва Людмила Анатоліївна – аспірант (Asieieva Ludmila Anatoliivna – postgraduate student). Phone:+380 (50) 160 93 83. E-mail: aseewal@i.ua.

Дата надходження
в редакцію: 13.05.2019 р.

Рецензент:
д.т.н., професор Вишнівський В.В.
Державний університет телекомунікацій, Київ