УДК 004.056:355.451

ІНФОРМАЦІЙНИЙ ЗАХИСТ ПЕРИМЕТРУ В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ БЕЗПРОВОДОВИХ МЕРЕЖАХ

Діденко Є.С.
Науковий керівник – к.т.н., проф. Марчук В.С.
Харківський національний університет радіоелектроніки, каф. ІКІ імені В.В.Поповського,
м. Харків, Україна
тел. +380(50)-168-14-18

This work is devoted to the study of information protection of the perimeter of wireless networks. In modern wireless networks, the traditional perimeter is transformed into a virtual one that goes beyond the physical. The network edge dynamically changes and passes through mobile devices and cloud infrastructure. The new model of access to information creates new threats. In this work, possible methods of protecting the virtual perimeter are studied.

Інформаційний захист периметру в сучасних телекомунікаційних безпроводових мережах залишається обов'язковим елементом інформаційної безпеки. Він дозволяє звести до мінімуму зовнішні загрози. Однак сучасні мережі не мають кордонів, Мобільність користувачів, необхідність обміну інформацією через зовнішні мережі, поява технологій хмарних обчислень і різноманітних хмарних сервісів вимагають нових підходів до захисту периметру.

Традиційний фізичний периметр перетворюється в віртуальний, що виходить за рамки об’єкта, що підлягає захисту. Захист фізичного периметру доводиться поширювати як за межі, так і в середину об’єкта. З розширенням способів доступу до інформаційних ресурсів і додатків у мережі більше немає єдиної точки входу. Нові технології вимагають інших підходів до організації захисту мережі.

Традиційний периметр зникає, йому на зміну приходить «нечіткий» периметр. Межа мережі динамічно змінюється і проходить по мобільних пристроях і хмарній інфраструктурі. Нова модель доступу до інформації породжує нові загрози, а значить, вимагає додаткових вимог до засобів захисту. Система захисту стає більш складною.

По-перше, потрібно забезпечити захист «класичного» периметра мережі. По-друге, захистити канали передачі інформації за допомогою технологій VPN для мобільних пристроїв. У віртуальних середовищах необхідне застосування віртуальних шлюзів безпеки.

Таким чином, треба контролювати все, що відбувається в мережі - зовні (в хмарі або на мобільних пристроях), на її межі, в центрах обробки даних, а також у внутрішній локальній мережі. Тільки за такої умови можна розраховувати на ефективний захист від цілеспрямованих і прихованих атак.

Для побудови ефективної системи безпеки необхідно визначити, яка інформація представляє цінність для організації, які сервіси і системи повинні бути доступні кінцевим користувачам, яким методам доступу організація віддає перевагу. Наступним кроком мають стати оцінка існуючого стану інформаційної безпеки і виявлення можливих ризиків. І вже виходячи з цього необхідно розробити концепцію та плани розвитку інформаційної структури мережі і системи інформаційної безпеки, Для рішення цієї задачі потрібно розгорнути систему моніторингу і контролю вхідного і вихідного трафіку на найвищих рівнях моделі OSI, щоб контролювати зміст інформаційних повідомлень і їх кореляцію з подіями безпеки.

Основними блоками в організації системи захисту будуть системи управління мобільними пристроями Mobile Device Management (MDM), додатками Mobile Application Management (MAM) і даними Mobile Information Management (MIM).

При цьому актуальність «класичних» механізмів захисту периметра не знижується. Це шлюзи безпеки Gateway (GW), засоби міжмережного екранування Fire Wall (FW), організація віртуальних приватних мереж Virtual Private Network (VPN), системи виявлення і запобігання вторгнень Intrusion Detection System/Intrusion Prevention System (IDS/IPS).

Більш того, розвиток мережних технологій призводить до подальшого розвитку елементів захисту. Наприклад, використовуються міжмережні екрани наступного покоління NGFW, що забезпечують багаторівневий захист на базі одного пристрою. Вирішувати питання забезпечення безпеки інформації необхідно системно і комплексно.

Все більшого значення набувають системи контентної фільтрації (URL-запитів та вхідного трафіку), як і раніце це важливий захист від спаму. Для захисту Web-додатків стають обов'язковими міжмережні екрани прикладного рівня (Web Application Firewall)».

Важливу роль в цьому відіграють надійні механізми захищеного доступу, в тому числі аутентифікація і захист даних, що передаються. Не менше значення має наявність єдиного центру управління доступом і розмежуванням прав користувачів.

Список використаних джерел:

1. Axel Buecker, Per Andreas, Scott Paisley. Understanding IT Perimeter Security. https://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf

2. Mallory Mooney. Best practices for network perimeter security in cloud-native environments. https://www.datadoghq.com/blog/securing-cloud-native-infrastructure-network-perimeter/