НАУЧНИ ТРУДОВЕ НА УНСС (3) 2022, ИК – УНСС
ISSN (online): 2534-8957; ISSN (print): 0861-9344; http://unwe-research-papers.org/
DOI: https://doi.org/10.37075/RP.2022.3.08

ПРЕДИЗВИКАТЕЛСТВА ЗА КИБЕРСИГУРНОСТТА ПРИ ИЗПОЛЗВАНЕТО НА ЛИЧНИ УСТРОЙСТВА В УНСС

Елица Павлова[1]
e-mail: epavlova@e-dnrs.org

Резюме

Доклада изследва предизвикателствата за киберсигурността при засилващата се тенденция „донесете вашето устройство“[2] и необходимостта от политика за нея. Тази политика е свързана с намаляване на риска при използването на лични устройства, като смартфони, таблети и лаптопи при осъществяване на достъп, получаване или използване на данни в мрежата на УНСС. Това е сложна област, поради наличието на множество потребители с различни устройства. Основните проблеми са увеличаването на кибер атаките, защитата на данните, контрола на достъп и управление на мобилните устройства. Целта на текста е да даде насоки за внедряване на политика и процедура за използването на лични устройства в УНСС, което ще спомогне да се запази поверителността, целостта и наличността на формационните активи на университета.

Ключови думи: киберсигурност, лични устройства, информационна сигурност, контрол на достъп

JEL: O30

Увод

Пандемията на COVID-19 ускори дигиталната трансформация и промени парадигмата за сигурност. Тя продължава да се разпространява в световен мащаб и много висши учебни заведения и научноизследователски организации преминаха към работа от дома, използвайки различни устройства за достъп до университетските системи, приложения и работни файлове. Осигуряването на сигурен достъп до всички тези ресурси е голямо предизвикателство. През 2020 г. от центъра по сигурност на Майкрософт (Microsoft Security, 2020) съобщиха, че образователната индустрия представлява 61% от 7,7 млн заплахи със злонамерен софтуер. Те са анализирали кибер рисковете, пред които са изправени университетите, както и необходимите предпазни мерки за сигурност, при работа в електронна среда.

[1] Докторант, катедра „Национална и регионална сигурност“, факултет „Икономика на инфраструктурата“, УНСС

[2] Използване на лично притежавано устройство, вместо да се използва официално предоставено.

Разрешаването на лични устройства за работа в университета и извън него има редица предимства, като повишено удовлетворение на служителите, подобрена производителност и спестяване на разходи. Основният проблем е, че използването им нарушава добрите практики за сигурност. Служителите използват лични смартфони, преносими компютри, таблети, външни дискове и безжични рутери, а често пъти те не са инсталирани с подходящия софтуер за защита на вътрешната мрежа. Това е свързано с редица проблеми за сигурността. Университетите трябва регулярно да оценяват своята кибер устойчивост и способността си да изпълняват учебните процеси, чрез комбинация от човешки усилия и информационни технологии.

Много университети по цял свят имат приети и публикувани политики за използването на лични устройства. Университета „Сейнт Джон“ прилага тази политика (Stjohns Edu, 2020) към университетската общност, като в нея включва „преподаватели, администратори, персонал, студенти, дипломирани/технически асистенти, възпитаници, стажанти, гости, външни лица и организации, осъществяващи достъп до мрежовите услуги на университета, както и други упълномощени потребители“. Университетът в Единбург (University of Edinburgh, 2021) признава предимствата от използването на собствени устройства за работа и определя минималните изисквания, на които те трябва да отговарят. В политиката на университета в Шефилд (The University of Sheffield, 2021) се казва, че той подкрепя персонала в практиката „донесете собствено устройство“, като гарантира, че продължава да контролира данните, за които е отговорен, независимо от собствеността на устройството, което е използвано за достъп до университетската мрежа. В раздела „Мониторинг на притежавани от потребителя устройства е записано, че „Университетът няма да наблюдава съдържанието на лични устройства, но си запазва правото да наблюдава и регистрира трафика на данни, прехвърлен между устройството и университетските системи“.

В статията „Защо киберсигурността трябва да бъде приоритет за образователния сектор“ се казва, че повече от 80% от всички кибер инциденти са причинени от човешка грешка (Swivel Secure, 2021). Образователните институции по цял свят губят милиони, възстановявайки се от инциденти, предизвикани от персонала. Необходими са добри програми за обучение по киберсигурност. Разбирането на служителите за това, което се крие зад всеки процес, е единственото, което може да изгради ефективна култура за кибер сигурност.

Данни за използването на лични устройства в УНСС

Всяко мобилно устройство, което съхранява университетски данни или има достъп до университетската мрежа, е потенциален източник на заплаха. Темата за сигурността на такива устройства засяга не само сигурния достъп до ин-

формационните ресурси, но и централизираното управление на политиките за мобилни устройства, използвани извън организацията. Разнообразието на тези устройства прави оценката на риска изключително трудна. За всяка операционна система съществуват различни опции за мрежова защита, което усложнява намирането на единно решение за сигурността. Друг потенциален проблем са преносимите дискове, тъй като много атаки могат да бъдат стартирани през тях.

Рисковете за сигурността включват:

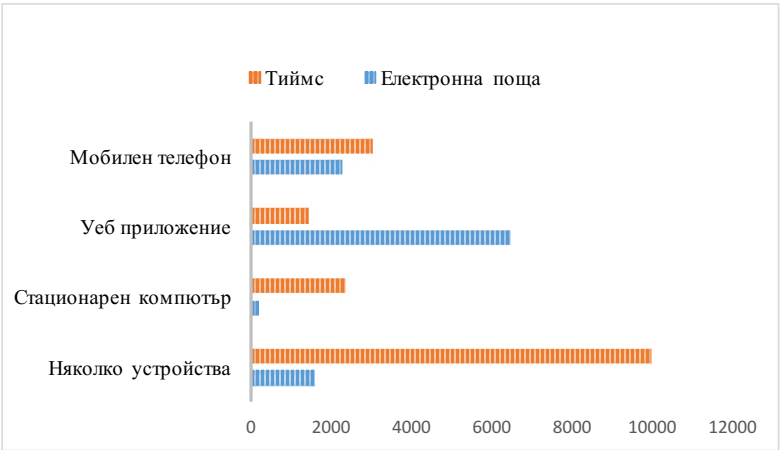
- Загуба на данни, които се предават, съхраняват и обработват на лично устройство, поради физическа загуба или кражба на устройство.
- Несигурна употреба, като свързване с незащитени безжични интернет мрежи или неприемливо използване на тези устройства от трета страна (приятели или семейство).
- Злонамерени приложения и вируси.

Съгласно препоръките на Европейската агенция по киберсигурност (ENISA Europa, 2021) за отдалечена работа, „всички корпоративни бизнес приложения трябва да са достъпни само чрез криптирани комуникационни канали“. Те препоръчват достъпът до порталите за приложения да бъде защитен чрез многофакторни механизми за удостоверяване и идентификация. Служителите трябва да разбират рисковете, които използването на собствени устройства в корпоративните мрежи може да причини, както и защо от тях се иска да спазват определени правила. „При използването на външни устройства, сигурността на данните зависи от служителите. Ако служител не изтегли актуализации на антивирусен софтуер и операционни системи, е възможно кибератака или проникване в мрежата през незащитеното устройство“ се казва в документа.

УНСС използва облачната услуга „Офис 365“ на Майкрософт, както и допълнителни инструменти за управление и защита срещу злонамерен софтуер и други видове атаки. Статистика от административния панел показва, че 27% от университетската общност, създава и споделя файлове в облака и те са достъпни от други устройства и по всяко време. Много малък процент споделят връзка към файл в облака, което прави споделянето по-сигурно и позволява на потребителите да си сътрудничат в реално време. Въпреки огромният брой онлайн занятия и конференции, само 46% използват възможностите на „Тиймс“ за комуникация. Когато хората могат бързо да се свържат с колеги и да получат достъп до имейлите и файловете си на всяко устройство, те са по-ефективни. Хората, използващи Майкрософт 365 на повече от едно устройство са близо 30%. Достъпът до файлове от всяко устройство спестява време, но само 24% се възползват от тази възможност.

Фигура 1 показва броят влизания на ден през мобилни телефони, уеб базирани приложения и персонални компютри в своя университетски мейл акаунт и платформата Тиймс. В университетската поща през повече от едно устройство влизат едва 15%, а за Тиймс този дял е 59%. Различните начини

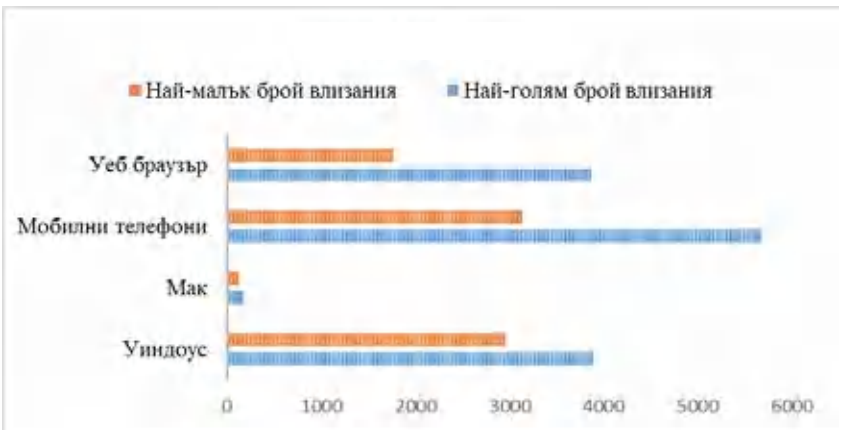
на комуникация показва как хората от университетската общност споделят знания и достъпват университетските ресурси.



Източник: Административния панел на „Офис 365“.

Фигура 1: Мобилност

Фигура 2 показва най-малкият и най-големият брой влизания за един ден в „Офис 365“ през различни платформи. Прави впечатление, че потребителите използват предимно мобилни телефони. Влизанията през уеб браузър и Уиндоус са почти еднакъв брой, както при минималните, така и при максималните стойности.



Източник: Административния панел на „Офис 365“

Фигура 2: Платформи

Университетът трябва да използва комбинация от официални политики за отдалечен достъп и мрежова сигурност, и да изискват от служителите да ги спазват, докато работят в университетската мрежа и извън нея.

Политики за използване на лични устройства

Политиката за използване на външни устройства трябва да очертае граница между работата и личния живот на служителите. Целите и условията, за които се допуска работа с такива устройства трябва да са дефинирани ясно. Преглед на редица университетски политики за сигурност на ИТ показва, че към всички устройства, свързани към мрежата на университета, има изискване те да бъдат регистрирани с потребителски акаунт и да имат актуализации на софтуера.

Процедурите за конфигурирането им се различават, както и отговорностите на ИТ отделите към тях. Техническата поддръжка за лично притежавани устройства в университетът в Единбърг (University of Edinburgh, 2021) е ограничена до „отстраняване на проблеми с мрежовата връзка, инсталиране на одобрени университетски софтуерни ресурси и конфигурация на виртуална частна мрежа, за да се позволи достъп до защитени ресурси с одобрение“. В някои университетски политики този раздел включва и списък с услуги, които не се поддържат от ИТ отдела. Отговорностите на потребителя включват: използване на антивирусен софтуер и защита на всички чувствителни данни, до които има достъп.

Правилата относно достъпа и забрана за изтегляне, копиране, прехвърляне или споделяне на чувствителна информация, обикновено са зададени в груповите политики на университета. Много университети са включили в политиката раздел „Рискове, задължения и отказ от отговорност“, в които се казва, че университетът не поема отговорност за поддръжката, архивирането или загубата на данни на лично устройство, както и че лицата нарушаващи политиката могат да бъдат подведени под отговорност за произтичащи щети.

Всички нарушения на информационната сигурност, действителни или предполагаеми, трябва да бъдат разследвани от директора по информационна сигурност[3] и докладвани на заместник ректора по електронизация[4]. Процедурата за реагиране в случай на изгубено или откраднато устройство, чрез която служителите биха могли да информират ИТ отдела за нарушения на сигурността, трябва да е детайлно описана. В нея трябва да фигурират отделите и лицата, които имат отговорности за сигурността на информаци-

[3] Използваното понятие „директор по информационна сигурост“ отговаря на длъжността CIS.

[4] Използваното понятие „заместник ректора по електронизация“ отговаря на длъжността CIO.

ята и ефективното прилагане на правилата и стандартите за информационна сигурност в рамките на университета.

За да се предотврати неоторизиран достъп, устройствата трябва да бъдат защитени с подходящи средства за автентификация и оторизация, като се използват функциите на устройството, а за достъп до университетската мрежа е необходима силна парола. Свързаността между политиките за информационна сигурност, управление на информацията, политиката за приемливо използване и политиката за управление на риска изграждат цялостната стратегия за киберсигурност.

Фигура 3: Свързани политики към политиката за използване на лично устройство

На фигура 3 са показани свързаните политики. Политиката за използване на лично устройство е част от правилата за приемливо използване и е предназначена да помогне на общността на университета да разбере своите отговорности при използване на информационните ресурси или мрежови услуги. Политиките за информационна сигурност се фокусират върху управлението и защитата на информация, която се обработва от служителите по време на тяхната работа. Тя включва реагиране на инциденти и контрол на достъпа. Политиката за управление на данни очертава рамка за класификация на данните и регламента за споделянето им.

Контрол на достъпа и управление на лични устройства

Нарастването на заплахите за сигурност на вътрешната информационно-технологична среда налага контрола на достъпа да се разглежда като технологична инфраструктура, която използва сложни инструменти, отразява промените в работната среда, като повишената мобилност, разпознава използваните устройства и отразява нарастващата миграция към облачните платформи. Повечето от нас работят в хибридни среди, където данните се придвижват от локални сървъри или от облака към учебни аудитории, офиси и домове с отворени безжични мрежи, което може да затрудни контрола върху достъпа. Тенденцията все по-голям набор от устройства да достъпват университетските мрежи, превръща създаването на постоянни политики в предизвикателство. Контролът, който селективно ограничава достъпа до данните се състои от два основни компонента – удостоверяване и оторизация. Удостоверяването само по себе си не е достатъчно. Необходим е и допълнителен слой за сигурност, който определя дали даден потребител трябва да има достъпа, които иска.

Определянето на подходящия модел за контрол на достъпа, който да отговаря на нуждите на конкретен университет, неговата структура и мисия, както и на вида и чувствителността на данните е много трудно.

Регистрирането на устройства в ИТ отдела помага да се наблюдават устройствата, свързани към мрежата. Администраторът може лесно да сравнява списък с регистрирани устройства със този на свързаните устройства. Днес най-разпространените модели за контрол на достъпа са базирани на ролята на потребителя[5] или базата на атрибути[6].

Експертите са единодушни, че организациите, които обработват данни за лична идентификация или други видове чувствителна информация, трябва да заложат контрол на достъпа като основа в архитектурата си за сигурност. Има различни видове софтуер за управление на мобилни устройства, позволяващ на ИТ отделите да управляват дистанционно устройствата на крайните потребители. Според сайта на Cisco (2020), те осигуряват заключване на устройството с ПИН; надеждна процедура за изтриване на всички данни в случай, че дадено устройство бъде откраднато, загубено или компрометирано по друг начин. Такова управление обаче, няма да бъде прието от университетската общност и това налага търсенето на други решения.

Външни безжични интернет рутери, които служителите свързват към университетската мрежата за собствено удобство са друг голям проблем. Паролите за тях се разпространяват между колеги и гости, в резултат на което достъпа до университетската мрежа става неконтролируем.

[5] Row Based Access Control (RBAC).

[6] Attribute Based Access Control (ABAC).

Контролът на достъп трябва да указват изискванията за достъп до университетската мрежа с външно устройство, както и отговорните за това лица. Определянето на класификационни нива на информация, спомага за определяне на изискванията за достъп. В политиките на Университета в Бостън е предвидено следното: „Изпълнителният директор[7], след консултация с отдела по сигурност, определя категориите чувствителна информация и подходящите предпазни мерки, необходими за защита на всяка категория. Стандартите за защита на данните определят административни, технически и физически предпазни мерки за защита на чувствителната информация. Отделът може да прегледа и изпълнителният директор да одобри стандартите за защита на данните“.

Определянето на подходящия модел, указващ изискванията за достъп до университетската мрежа с лично устройство, както и отговорните за това лица е свързано с редица управленски решения.

Различните видове софтуер за управление на мобилни устройства са неприложими, защото достъпа до лични устройства и тяхното дистанционно управление няма да бъде прието добре от университетската общност. Внедряването на мрежово базирано решение за откриване на заплахи ще спомогне за наблюдение на цяла защитена мрежа и свързаните към нея устройства, без да натоварва потребителите. Контролът на достъп трябва да изисква двуфакторно удостоверяване за всички потребители.

Възможности за внедряване на единен вход

УНСС има защитна стена, която осигурява интегрирана защита срещу заплахи за целия процес на атаката във всяко устройство.

Нейните възможности включват (Cisco, 2020):

- Сигурен отдалечен достъп за непрекъснатост на процесите.
- Видимост и контрол на приложенията и оптимизиране на ефективността на сигурността.
- Филтриране на уеб адреси и налагане на политики за тях в повече от 80 категории.
- Откриване на пробиви, зловреден софтуер и възникващите атаки.

Защитната стена и модула към нея предоставят на администраторите цялостна видимост и контрол върху дейността в мрежата. Това включва потребители, устройства, комуникация между виртуални машини, уязвимости, клиентски приложения, файлове и уеб сайтове, както и централизирано управление на работния процес на мрежовите операции. Модулът интегрира голям набор от възможности: управление на политики и обекти,

[7] Отговаря на длъжността Chief Information Officer в модела КОБИТ.

управление на събития, отчитане и отстраняване на неизправности за функциите на защитната стена.

Използването на възможностите на този модул ще реши проблемите, произтичащи от използването на лични устройства във вътрешната мрежа на УНСС. Ползите от него биха били: предотвратяване и смекчаване на кибер заплахите; откриване, блокиране, проследяване, анализ и отстраняване на целенасочени и постоянни атаки от зловреден софтуер; прилагане на правила, основани на пълна видимост на потребители, мобилни устройства, клиентски приложения, комуникация между виртуални машини, уязвимости, заплахи и уеб адреси; подробни отчети за киберзаплахи; по-ниски оперативни разходи и административна сложност, автоматична настройка на политиката за сигурност и идентификация на потребителя.

Процедурата за използване на лично устройство е неразделна част от политиката и трябва да включва попълването на електронен формуляр, съдържащ информация за потребителя, контакти, дирекция / отдел / факултет / катедра, към която работи, заемана длъжност; технически параметри на личното устройство; желан достъп до определени информационни ресурси; продължителност на използване и декларация за информираност относно политиката за използване на лични устройства.

Организирането на целия процес е свързано с редица управленски решения. Ролите и организационни структури, които отговарят за сигурността са описани в модела КОБИТ[8]. Най-отгоре в йерархията е съвета от най-висшите ръководители и/или изпълнителни директори, отговорни за управлението и цялостния контрол на информационните ресурси. Този съвет докладва на ректора и включва: главен изпълнителен директор[9], оперативен директор[10]; директор, отговорен за всички аспекти на управлението на риска[11]; директор информационни технологии[12], отговорен за управлението на информационните ресурси, услуги и решения; технологичен директор[13] и главен служител по сигурността на информацията[14].

[8] COBIT® 2019.
[9] Отговаря на длъжността Chief Executive Office от модела на КОБИТ.
[10] Отговаря на длъжността Chief Operating Officer от модела на КОБИТ.
[11] Отговаря на длъжността Chief Risk Officer от модела на КОБИТ.
[12] Отговаря на длъжността Chief Information Officer от модела на КОБИТ.
[13] Отговаря на длъжността Chief Technology Officer от модела на КОБИТ.
[14] Отговаря на длъжността Chief Information Security Officer от модела на КОБИТ.

Заключение

Поддържането на инфраструктура, която гарантира мрежовата и информационната сигурност, е основен приоритет на Университета за национално и световно стопанство. Създаването на строги правила за контрол на достъпа, които потребителите не могат да променят без одобрение от администратор, е определящо за нивото на сигурност. Политиката за използване на лично устройство, трябва да описва целите и условията, при които се допуска работа със собствени устройства в университетската мрежа и извън нея. Прилагането й трябва да бъде обвързано с процедура за действие и обучение, за това как да се прилагат методите за сигурност и каква е необходимостта от тях.

Често използваните контроли за достъп не отговорят напълно на изискванията за сигурен достъп до вътрешната мрежа и неговите ресурси. След направен анализ на предизвикателствата пред сигурността при използването на лични устройства, като най-добър избор е предложено използването на съществуващия модул към защитната стена. Той включва контрол на достъпа върху потребители, устройства, комуникация между виртуални машини, уязвимости, заплахи, клиентски приложения, файлове и уеб сайтове, както и централизирано управление на работния процес на мрежовите операции. Конфигурирането му изисква цялостен поглед върху информационната сигурност и стратегическите цели на университета. Насоките на Агенцията на Европейския съюз за киберсигурност, могат да бъдат адаптирани и приложени в процеса на работа.

Използван литература

Cisco (2020). Mobile Device Managers for BYOD, Cisco, available at: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_MDMs.html (accessed 2.1.21)

Cisco. (2020). Cisco ASA with FirePOWER Services, Cisco, available at: https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html (accessed 2.17.21)

ENISA Europa. (2021). Security is key for BYOD.

Microsoft Security. (2020). Security intelligence, Microsoft Security, available at: https://www.microsoft.com/security/blog/security-intelligence/ (accessed 2.1.21)

Stjohns Edu. (2020). Bring Your Own Device (BYOD) Policy, Stjohns Edu, available at: https://www.stjohns.edu/about/administrative-offices/human-resources/policy-911-bring-your-own-device-byod-policy (accessed 2.2.21)

Swivel Secure. (2021). Why Cybersecurity Needs To Be a Priority for The Education Sector, Swivel Secure, available at: https://swivelsecure.com/solutions/education/why-cybersecurity-needs-to-be-a-priority-for-the-education-sector/

The University of Sheffield. (2021). The University of Sheffield, available at: https://www.sheffield.ac.uk/ (accessed 2.16.21)

University of Edinburgh. (2021). BYOD Policy, available at: https://www.ed.ac.uk/infosec/information-protection-policies/information-security-required-reading/byod-policy (accessed 2.1.21)

***

CHALLENGES FOR CYBER SECURITY IN THE USE OF PERSONAL DEVICES AT UNWE

Elitsa Pavlova, PhD Candidate
Department of National and Regional Security
Faculty of Infrastructure Economics
University of National and World Economy
e-mail: epavlova@e-dnrs.org

Abstract

The report explore the challenges of cybersecurity in the growing trend of „bring your own device" and the need for a policy for it. This policy is related to reducing the risk of using personal devices, such as smartphones, tablets and laptops when accessing, receiving or using data in the UNWE network. This is a complex area due to the presence of multiple users with different devices. The main problems are the increase in cyber attacks, data protection, access control and management of mobile devices. The purpose of the report is to provide guidelines for the implementation of a policy and procedure for the use of personal devices at UNWE, which will help preserve the confidentiality, integrity and availability of the university's formation assets.

Key words: cybersecurity, personal devices, information security, access control

JEL: O30