РЕГЛАМЕНТ

ЗА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ ПЛОВДИВСКИ УНИВЕРСИТЕТ „ПАИСИЙ ХИЛЕНДАРСКИ“

26.08.2020

1. ПРЕАМБЮЛ

Мерките за мрежова и информационна сигурност, разписани в този документ са организационни, технологични и технически и се прилагат в съответствие с Постановление 186 на МС от 19 юли 2019 г. [1] и отразяват утвърдени добри практики за изграждане на университетска мрежа [2]. Документът обхваща основните цели на мрежовата и информационната сигурност, запазване на достъпността, интегритета и конфиденциалността на информацията по време на целия ú жизнен цикъл в Пловдивския университет.

2. ИНФОРМАЦИОННА СИГУРНОСТ

A. Разпределение на роли и отговорности

Ректорът на Пловдивския университет и Директорът на Университетския Информационен Център (УИЦ) пряко отговарят за информационната сигурност, в това число и физическата сигурност на информационните и комуникационни системи на Пловдивския университет. Териториалните подструктури и разпределени информационни системи се управляват от служители, отговорни за сигурността им, като те се координират от Дирекоторът на УИЦ.

B. Политика за сигурност

Основният документ, дефиниращ вътрешната политика за информационна и мрежова сигурност е „Вътрешни правила за работа с информационните системи и контролни дейности, свързани с информационните технологии“ [file01.pdf], който се актуализира периодично. В него подробно са разписани структурата и използването на информационните ресурси, видове рискове и заплахи, организацията за достъп до информацията и оторизация, контрол върху отделните дейности и дисциплинарни отговорности.

Повишаването на квалификацията на отговорните екипи се реализира чрез периодични вътрешни и външни семинари и обучения.

C. Документирана информация

УИЦ и териториалните подструктури водят надлежна документация, еднозначно идентифицирана чрез заглавие и име на файл, субект на действие, версия, дата, номер и автори. Документацията се поддържа в актуализирано състояние и се одобрява от Директора на УИЦ или ръководителите на подструктури. Съответната файлова информация е достъпна само до отговорните лица и се предоставя на представители на съответните национални компетентни органи съгласно чл. 16, ал. 5 от Закона за киберсигурност при нужда: опис на информационните активи [file02.pdf], физическа схема на свързаност [file03.pdf], логическа схема на информационните потоци [file04.pdf], документация на структурната кабелна мрежа и подмрежи [file05.pdf], техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти [file06.pdf], и инструкции и вътрешни правила за администрирането, експлоатацията и поддръжката на хардуер и софтуер [file07.pdf].

D. Класификация на информацията

По отношение на мрежовата и информационна сигурност, информацията се дефинира в няколко типа. По смисъла на TLP (traffic light protocol) се въвеждат кодовете червено (TLP-RED), жълто (TLP-AMBER), зелено (TLP-GREEN) и бяло (TLP-WHITE):

i. Ниво 0, TLP-WHITE: публична и общодостъпна информация и документи, публикувани на сайта на Пловдивския университет и/или на специализираните сайтове на основни звена;

ii. Ниво 1, TLP-GREEN: вътрешна информация до отдели, комисии, звена или група от потребители;

iii. Ниво 2, TLP-AMBER: чувствителна информация за студенти, преподаватели и външни лица и организации, в това число проверка на идентичност, електронен подпис, мрежови системи, съдържащи данни за адресация и маршрутизация. Данните от Ниво 2 се предават задължително по надежден начин, в криптиран вид.

iv. Ниво 3, TLP-RED: тази информация не се разпространява, като информационните потоци са сведени само до отговорните лица за управление на услуги и комуникации.

Детайлното класифициране на информацията е описано в документ [file08.pdf], според който следва да се прилагат политиките за разпространение описани по-горе.

E. Управление на риска

Всяка година, а при нужда и по-често се извършва анализ и оценка на риска по предварително изготвена методика [file09.pdf], одобрена от Директора на УИЦ. На оценка се подлагат всички информационни, комуникационни и мрежови ресурси, както и вътрешните и външни условия на работа на отговорните лица.

F. Управление на информационните активи

Според вътрешните правила за техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти (file06.pdf) се описват всички активи с инвентарен номер, основни характеристики, работни потоци, в които участва актива, местонахождение, година на производство, свързана с него документация и отговорни за софтуерното и хардуерното му състояние.

G. Сигурност на човешките ресурси

С цел намаляване на инциденти поради човешка грешка се провеждат два типа обучения на персонала – външни обучения и регулярни вътрешни семинари и инструктажи. Инструктажите се провеждат по утвърден от Директора на УИЦ график, като се пази история на изминалите събития с възможност за проследяване [file10.pdf].

H. Взаимодействия с трети страни

При получаване на стоки и услуги от трети страни, Пловдивският университет съблюдава и изисква гаранция за мрежова и електронна сигурност както по отношение на предоставяните стоки и услуги, така и до достъпа до вътрешни ресурси. Взаимодействието с трети страни се удостоверява, чрез подписване на договор по отношение на качество и срокове, които могат да създадат риск в сигурността.

I. Управление на измененията в информационните активи

Документът file07.pdf съдържа подробни инструкции и вътрешни правила за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер. Преди всяка промяна на активи (информационни и мрежови) се извършва анализ и оценка на риска. Като промените се съгласуват с Директора на УИЦ и оповестяват три дни предварително съгласно класификация на информацията.

J. Сигурност при разработване и придобиване на информационни и комуникационни системи

Въвеждане, интегриране, разработка и придобиване на информационни и комуникационни системи се извършва след анализ и оценка на риска, с цел да се гарантира, че ниво на сигурност на информацията, мрежите и информационните системи според заложеното в етапа на разработка. Всички тестове се документират за доказателство на защитата на информацията от загуба на достъпност, интегритет и конфиденциалност.

3. ЗАЩИТА

A. Сегрегация

Принципа за сегрегация се прилага на няколко нива в Пловдивския университет: (1) чрез териториални подструктури, характеризиращи се с обособени подмрежи и информационни ресурси (сървъри, маршрутизатори), (2) във всяка подструктура са обособени физическо

(сървъри и маршрутизация) и логическо (виртуализация) разделяне на услугите и ресурсите и (3) системи и услуги на трети страни са отделени логически от университетската инфраструктура. Многослойните системи и услуги, ползващи сървъри за уеб, база данни и приложно-програмни интерфейси се разполагат на различни хардуерни машини и в различни мрежи.

B. Филтриране на трафика

Филтрува се неизползваният IPv4 и IPv6 трафик по протоколите UDP и TCP до всички налични подмрежи: сървъри, инфраструктура, потребители и териториални подструктури. Правилата за филтруване са предварително разписани в документ [file11.pdf] и одобрени, като се актуализират периодично.

C. Неоторизирано използване на устройства

На територията на Пловдивския университет право на достъп до интернет имат лични технически устройства, вкл. и преносими записващи устройства, собственост на студенти, преподаватели, служители и гости на университета. Достъпа до мрежата и интернет е безжичен, като се прилагат допълнителни филтри. Достъпа до вътрешни ресурси е само от Ниво 0 (TLP-WHITE).

D. Криптография

Университетът разполага с криптографска политика, синхронизирана с нормативните и регулаторните изисквания за съхраняване и пренасяне на информация.

E. Администриране на информационните и комуникационните системи

Административните профили на всички устройства в мрежата отговарят на следните условия:

1. Променени идентификационни данни от производител или доставчик;
2. Всеки административен профил е персонален;
3. Всеки административен профил се използва само за административни цели;
4. Всеки администратор разполага с административни права съобразени с изпълняваните от него задачи и не по-високи;
5. Администраторските акаунти са различни за всяка система и се пазят в криптиран вид в сейф, като физическия и логически достъп до тях се осъществява от минимум 3 служители на УИЦ (в т.ч. Директорът на УИЦ).
6. Поддържа се списък с всички профили и съответните услуги и устройства, които се администрират чрез тях;
7. Акаунти, които не се използват активно се деактивират;

8. Ежегодно се проверява актуалността на административните профили.

Паролите на административните акаунти се променят задължително при:

1. Промяна на договорни отношения на служители или трети страни, на които са били известни паролите;
2. При пробив в мрежовата или информационна сигурност;
3. Ежегодно се променят всички администраторски пароли.

F. Среда за администриране

Административните интерфейси на всички мрежови и информационни ресурси са достъпни от витруална частна мрежа, която не е достъпна за други потребители. Достъпа до тази мрежа е възможен чрез персонален VPN достъп.

G. Управление на достъпите

Териториалните подструктури, потребителите или информационните и мрежови системи на Пловдивския университет при строга необходимост получават достъп до информационните и комуникационни системи за изпълнение на техните задължения или безпроблемна работа на автоматизираните процеси. За целта се дефинират специфични права за достъп, прилага се оторизация и автентикация, паролите за достъп са поне от 9 символа, съдържащи малки и големи букви, цифри и специални символи, като се променят най-малко един път на шест месеца. Университетския и информационен център гарантира, че достъпа до тези ресурси е ограничен само от вътрешната мрежа.

H. Защита при отдалечен достъп/работа от разстояние

Отдалечен достъп до информационните ресурси на Пловдивския университет е реализиран чрез двуфакторна автентикация или VPN достъп, като са ограничени ползването на FTP или RDC (Remote Desktop Connection).

I. Защита на хардуерни устройства

УИЦ и териториалните информационни подструктури предлагащи услуги, с цел намаляване риска от инциденти, поддържат климатизирани помещения с постоянен мониторинг на физичните параметри на средата, сензорните показания и останалите параметри на системите. Провежда се периодична профилактика. Достъпа до помещенията е оторизиран, като се регистрира всяко посещение в тях.

J. Защита на софтуер и фърмуер

Използваните системи софтуери и фърмуери трябва да бъдат поддържани от производителя/разработчика, като винаги се използват последните им стабилни версии. За целта се поддържа Библиотека с дистрибутиви на използвания софтуер и фърмуер [file12.pdf]. Библиотеката също така съхранява offline копия на моментно инсталираните версии и текущи конфигурации. Периодично се следи за нерагламентирани промени, по

възможност се прави абонамент към производителя за нови версии или известни уязвимости. Прилагат се периодично ъпдейти.

K. Защита от зловреден софтуер

Защитата от зловреден софтуер се реализира в две направления (1) абонамент и следене на известни актуални уязвимости в това число бюлетина на Националният Център за Действие при Инциденти в Информационната Сигурност и (2) следене състоянието на системите поне веднъж седмично и вземане на съответните мерки спрямо Политиката за мрежова и информационна сигурност.

L. Защита на уеб сървъри

Използваните публично достъпни уеб сървъри, представляващи Пловдивският университет отговарят на утвърдените стандарти за пренос на данни, а именно: инсталира се сертификат на уеб сървърите, издаден от доверена система за сертифициране (trusted certification authority system). Сертификатът трябва да е издаден за съответния уеб сайт (website) или група сайтове и да е уникален, да използва алгоритъм за криптиране поне SHA2 и да е актуален, като сертификатите с изтекъл срок се анулират. Достъпът до съдържание се реализира само по протокол Hypertext Transfer Protocol Secure (HTTPS), като се използват само криптографски транспортни протоколи TLS (Transport Layer Security) версия 1.2, дефиниран в RFC 5246 на IETF [3], версия 1.3, дефиниран в RFC 8446 на IETF [4], или следващи по-нови версии. С цел предотвратяване на кибер атаки от тип Cross-Site Request Forgery (CSRF), Cross-site Scripting (XSS), file inclusion, SQL injection и др. се прилага подходящ Web Application Firewall. който наблюдава и филтрира трафика от и към съответното приложение. С цел защита от DoS атака, сървърите се конфигурират с определен лимит на заявките до тях в зависимост от очакваната натовареност на сървъра, прилагат се и ограничения за времетраенето на връзката. В случаите на уеб оторизация е въведен лимит на броя неуспешни опити за влизане в системата. Инструкции към индексиращите роботи се поставят във файл robot.txt на всеки сайт. Системите за управление на съдържанието (CMS) се конфигурират според препоръките на разработчиците, в това число промяна на директории по подразбиране, потребителски акаунти и т.н.

M. Защита на Domain Name System (DNS)

Домейнът на Пловдивският университет е UNI-PLOVDIV.BG. Този и другите използвани от университета домейни и поддомейни отговарят на условията: всеки оторитивен за даден домейн сървър се разполага в различна мрежа, прилагат се DNSSEC стандартите, забранява се свободния трансфер на зоните, прилагат се лимити за достъп до сървърите с цел предотвратяване на злонамерен достъп. Конфигурират се SPF и dmarc записи.

N. Физическа сигурност

Прилагат се мерки с цел физическа защита на информационните активи, които гарантират наличността, интегритета и конфиденциалността на данните и услугите. Към всеки териториален център за колокация се прилага процедура за защита на данните в случай на бедствие (пожар, наводнение, химическа и физическа промяна на средата). Извършва се постоянно видеонаблюдение и се организира проследимост на достъпа.

O. Наблюдение

Всички мрежови и информационни устройства се наблюдават непрекъснато, като информационните им потоци, протоколи и файлове се подлагат на анализ с цел предотвратяване на инциденти.

P. Системни записи (logs)

Всички мрежови и информационни устройства поддържат единно време чрез конфигуриран NTP протокол. Всяко едно събитие се записва на отдалечен LOG сървър, разположен в не публична мрежа. Колекционираните системни записи се анализират за инциденти, като те се докладват на ангажираните отговорни лица.

Q. Управление на инциденти с мрежовата и информационната сигурност и уведомяване за инциденти

Дейностите по обработка на сигнали и реакция при инциденти са разписани в file07.pdf. В случай на инциденти се прилагат правилата за споделяне на информацията със служители, партньори, доставчици, клиенти, медии, държавни органи, разписани в file13.pdf.

4. ВЪТРЕШНА ДОКУМЕНТАЦИЯ

A. file01.pdf:: Вътрешни правила за работа с информационните системи и контролни дейности, свързани с информационните технологии

B. file02.pdf:: Опис на информационните активи

C. file03.pdf:: Физическа схема на свързаност

D. file04.pdf:: Логическа схема на информационните потоци

E. file05.pdf:: Документация на структурната кабелна мрежа и подмрежи

F. file06.pdf:: Техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти

G. file07.pdf:: Инструкции и вътрешни правила за администрирането, експлоатацията и поддръжката на хардуер и софтуер

H. file08.pdf:: Класификация на информацията

I. file09.pdf:: Методика за анализ и оценка на риска

J. file10.pdf:: График на инструктажите за повишаване сигурността на човешките ресурси

K. file11.pdf:: Правила за филтриране на трафика

L. file12.pdf:: Библиотека с дистрибутиви на използвания софтуер и фърмуер

M. file13.pdf:: Стратегия за комуникация в случай на инциденти

5. ВЪНШНИ ПРЕПРАТКИ

1. Постановление № 186 от 19 юли 2019 г. за приемане на Наредба за минималните изисквания за мрежова и информационна сигурност, https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=139834

2. Campus Best Practice, https://services.geant.net/sites/cbp/Pages/Home.aspx

3. The Transport Layer Security (TLS) Protocol Version 1.2, https://tools.ietf.org/html/rfc5246

4. The Transport Layer Security (TLS) Protocol Version 1.3, https://tools.ietf.org/html/rfc8446

5. DNS Security Introduction and Requirements, https://tools.ietf.org/html/rfc4033