Киберсигурност във висшите училища – подходи и добри практики

Габриела Наскова

Cybersecurity in higher education - approaches and good practices

Gabriela Naskova

Abstract:

As a consequence of the developing world and the European directives on the digitization of education, higher schools increasingly rely on digital technologies. This puts them at constant risk of cyber-attacks.

Securing endpoints, including laptops, PC, and more, is becoming a core task of any higher school's cybersecurity strategy. ESET Endpoint Protection is a popular solution widely used in various organizations. The advantages and opportunities in a university environment are discussed.

The system is easy to implement, which is a crucial consideration for universities, which in Bulgaria often have limited IT resources. ESET Endpoint Protection is effective at detecting and preventing a range of cyber threats, including malware, phishing attacks and ransomware. The software collects data on endpoints and offers graphs to analyze the behavior of each. As a result of the factors described above, the system was chosen as part of the cyber security strategy of UNWE.

Keywords: cybersecurity, higher education, specialized software, endpoints, cyber threats

For contacts: Gabriela Naskova, University of National and World Economy, Sofia, Bulgaria, gnaskova@unwe.bg

ВЪВЕДЕНИЕ

В следствие от развиващия се свят и европейските директиви за дигитализация на образованието, висшите училища все повече разчитат на цифрови технологи. Това ги изправя непрекъснато пред голям риск от кибератаки.

Осигуряването на защита на крайните станции, включващи лаптопи, настолни компютри и мобилни устройства от киберзаплахи се превръща в основна задача от стратегията за киберсигурност на всяко висше училище, която поставя и голямо предизвикателство заради разнообразната дейност и специфичните нужни на всяка образователна институция.

Основните усилия във висшите училища в България по темата за киберсигуростта са насочени към удовлетворяване на изискванията на Наредбата[18] за минималните изисквания за мрежова и информационна сигурност, приета с ПМС № 186 от 26.07.2019 г., обн., ДВ, бр. 59 от 26.07.2019 г., в сила от 26.07.2019 г. Наредбата служи за отправна точка за повишаване на нивото на защитата срещу инциденти, рискове и заплахи за мрежовата и информационната сигурност в Република България, с което засяга пряко висшето образование в страната.

С оглед на посоката на развитие, през 2022 г. в Университет за национално и световно стопанство е приета „Стратегия за дигитализация на УНСС 2022-2025“.

Стратегията за дигитализация указва редица насоки за системна работа в областта на киберсигурността. Наред с нормативните изисквания са отчетени и добрите практики на водещите компании, особено в сложната съвременна

[18] НАРЕДБА за минималните изисквания за мрежова и информационна сигурност

геополитическа ситуация. Целите и очакванията за силна дигитализация на приложенията, процесите и услугите в УНСС излагат на много висок риск информационната инфраструктурата, ако не са предприети необходимите мерки за киберсигурност.

ESET Endpoint Protection е популярно решение за защита на крайните точки, което се използва широко в различни организации. В доклада се разглежда системата в университетска среда като е обърнато внимание на общите ползи от внедряването и разгледан пример от реалната среда.

ИЗЛОЖЕНИЕ

Сигурността на крайните точки се очертава като критичен компонент от стратегията за киберсигурност на висшите училища, което включа защитата от киберзаплахи като злонамерен софтуер, фишинг атаки и рансъмуеър.

Дигиталната инфраструктура на УНСС е изцяло съобразена със съвременните технологични изисквания и нейното развитие е ключов елемент на процесите на електронизация на всички нива като основен акцент се поставя на учебната дейност и научноизследователска дейност. Политиката на дигитализация на средата за обучение в УНСС е фокусирана върху:

1. подобяване на сървърните системи и компютърните конфигурации;
2. постоянен мониторинг на информационната инфраструктура
3. съответстващо поддържане на системното софтуерно осигуряване и др.

Една от основните дейности за постигане на високо ниво на киберсигурност в Университета на национално и световно стопанство е закупуването и въвеждането в експлоатация на софтуер за защита на крайните точки, а именно Endpoint Security (ESET).

ESET Endpoint Protection предлага набор от функции и възможности, които го правят подходяща система за прилагане в различни по формат и предназначение организации.

Софтуерът включва усъвършенствани механизми за откриване и предотвратяване на заплахи, като машинно обучение и откриване, базирано на поведение. Той също така разполага с вградена защитна стена, която може да помогне за блокиране на неоторизиран достъп до крайните точки. В допълнение, ESET Endpoint Protection предлага набор от функции за управление като отдалечено внедряване, управление на политики и отчитане, които могат да опростят управлението на крайни точки в университетска среда.

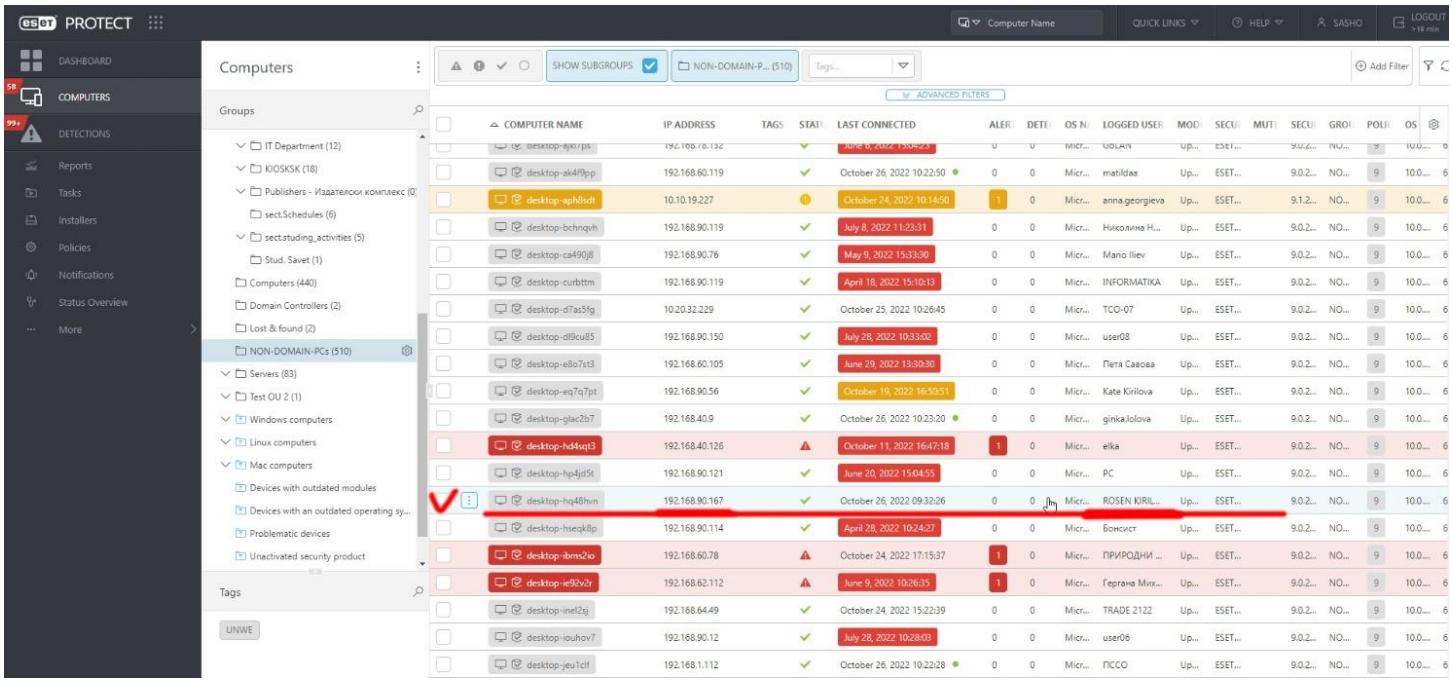
Внедряването на решения за сигурност на крайните точки може да повлияе на ИТ инфраструктурата на висшено училище, включително на производителностите на мрежата и крайните точки, което пък от своя страна рефлектира върху потребителското изживяване. ESET Endpoint Protection обаче е проектиран да има минимално въздействие върху крайните точки и производителността на мрежата. Софтуерът е лек и използва минимални системни ресурси, с което се гарантира, че крайните точки продължават да функционират на оптимални нива. ESET Endpoint Protection е проектиран да работи във фонов режим, без да прекъсва работата на потребителя.

ESET Endpoint Protection е проектиран да бъде лесен за внедряване и управление, което го прави подходящ избор за висшите училища. Софтуерът

включва функции за автоматизирано внедряване и конфигуриране, които могат да помогнат за намаляване на времето и усилията, необходими въвеждане на системата в действие.

В допълнение, ESET Endpoint Protection включва редовни актуализации и корекции, за да гарантира, че софтуерът остава актуален с най-новите заплахи и уязвимости.

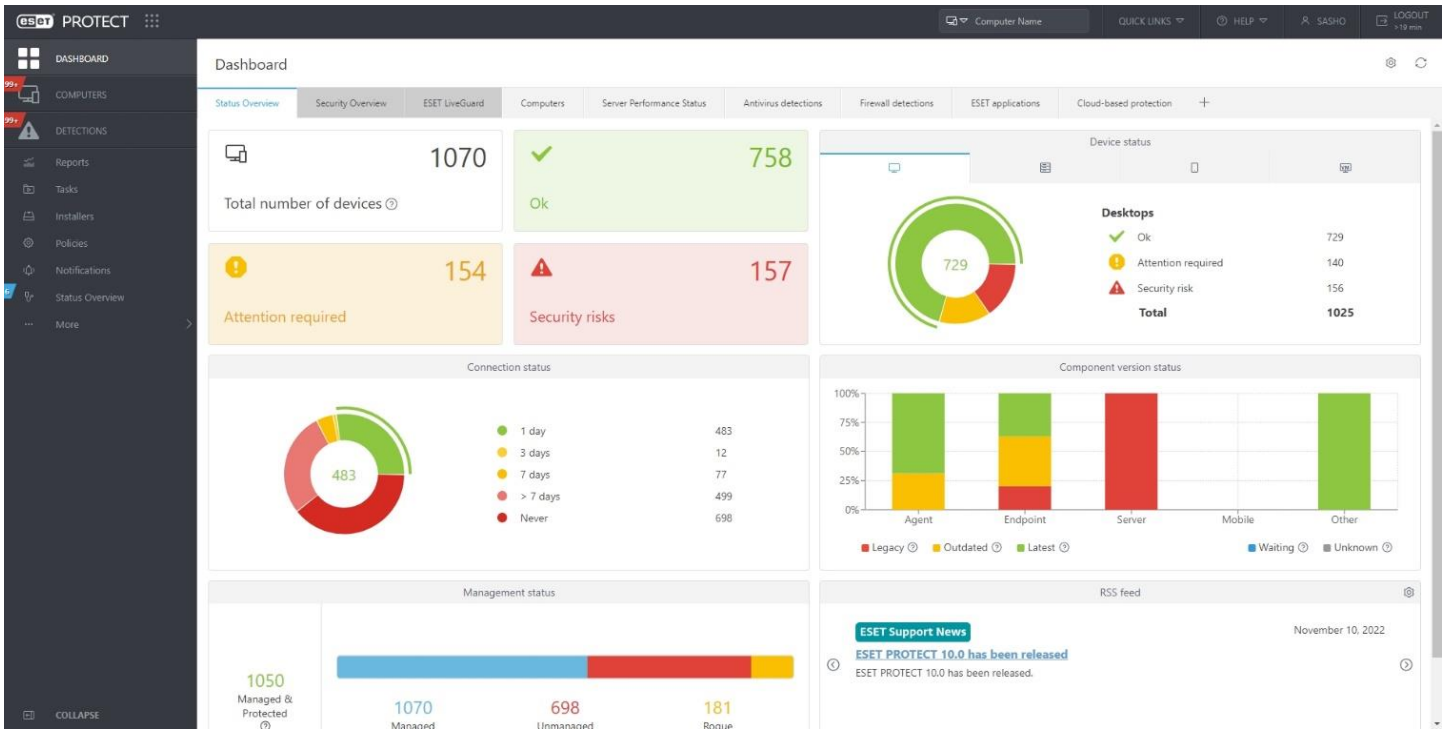
Предложен е удобен за потребителите интерфейс *(фиг. 1)*, с който се улеснява управлението на защитата на крайните точки и предлага графики за анализ на поведението.



Фиг. 1. Списък на крайните точки в УНСС

На фиг. 1 е визуализиран екран в ESET Endpoint Protection, на който са изброени крайните точки в УНСС със съответните им имена. В зависимост от цвета, в който са оцветени, администраторът може лесно да се ориентира за нивото на заплаха: при червен цвят значи е открита заплаха, при оранжев – станцията трябва да бъде под наблюдение. Колона „Alert” посочва броя на заплахите.

При избор на конкретна крайна точка, се извежда меню с подробна информация за характеристиките ѝ и моментното състояние на конфигурацията.



Фиг. 2. Табло за анализ в ESET Endpoint

На фиг. 2 е показано табло за анализ на общото състояние на крайните точки в компютърната система – в случая на разглеждания пример с УНСС. Визуализира се общият брой устройства, колко от тях са под заплаха, при кои софтуерът се нуждае от ъпдейт. Налични са и други критерии за анализ.

В УНСС чрез въвеждането на работата с ESET Endpoint Protection се постига:

- ✓ общо подобряване на сигурността в инфраструктурата на УНСС;
- ✓ отчетност за състоянието на работните станции и сървъри;
- ✓ възможност за налагане на различни политики за сигурност;
- ✓ известяване в случай на malware outbreak;
- ✓ създаване на различни динамични групи за изпълнение на задачи, свързани със сигурността;
- ✓ ролево базиран достъп на администраторите;
- ✓ подробни доклади за състоянието на работните станции и сървъри и др.

ЗАКЛЮЧЕНИЕ

Информационните и комуникационни технологии са основен лост за цифровата революция в Европа – от умните крайни точки до свръхскоростния интернет, мобилните приложения и научните изследвания в областта на бъдещите и нововъзникващи технологии. Технологиите са и основополагащ фактор за изграждането на конкурентоспособна икономика, основана на знанието. Висшите училища, в стремежа си да отговарят на нуждите в съвременния свят, разполагат със знание за хиляди хора – техните потребители в лицето на бивши, настоящи и потенциални обучаеми, преподаватели и служители – под формата на лични данни, потребителско поведение, досиета и други. Това ги прави отговорни да пазят и управляват тази информация така, че тя да не попада под заплаха от неоторизиран или зловреден достъп.

ESET Endpoint Protection е подходящо решение за сигурност на крайни точки за университети, които искат да подобрят позицията си по отношение на киберсигурността.

ESET Endpoint Protection е проектиран да има минимално въздействие върху ИТ инфраструктурата, лесен е за внедряване и управление и е ефективен при откриване и предотвратяване на кибератаки.

Въпреки че никое решение за сигурност на крайни точки не може да предложи пълна защита срещу всички киберзаплахи, ESET Endpoint Protection е ценен инструмент в набора от инструменти за киберсигурност на университета.

ЛИТЕРАТУРА

1. НАРЕДБА за минималните изисквания за мрежова и информационна сигурност - http://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=139834
2. Министерство на електронното управление
3. Национална програма „Цифрова България 2025“
4. Вътрешни документи на УНСС
5. www.eset.com
6. www.unwe.bg