

Как защитить учебные заведения в эпоху тотальной цифровизации

2023

Сегодня

- Онлайн-платформы обучения
- Многообразие устройств
- Терабайты данных

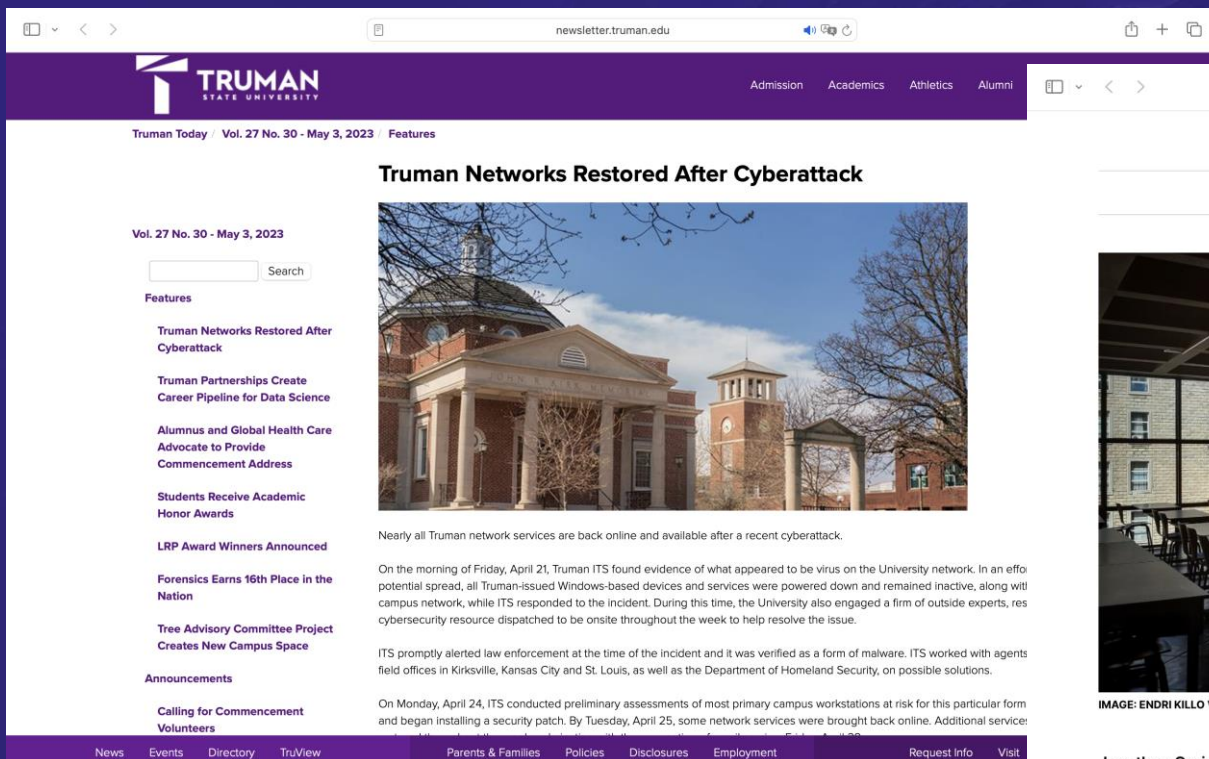


Что опасней, взломать машину или взломать человека?



Кибер-атаки, это не всегда про деньги!

Взломы учебных заведений уже не новость



Truman State University newsletter page. The header includes the university logo and navigation links for Admission, Academics, Athletics, and Alumni. The main content area features the article "Truman Networks Restored After Cyberattack" with a search bar and a list of featured articles on the left. The article text describes the restoration of network services after a cyberattack on Friday, April 21, 2023.

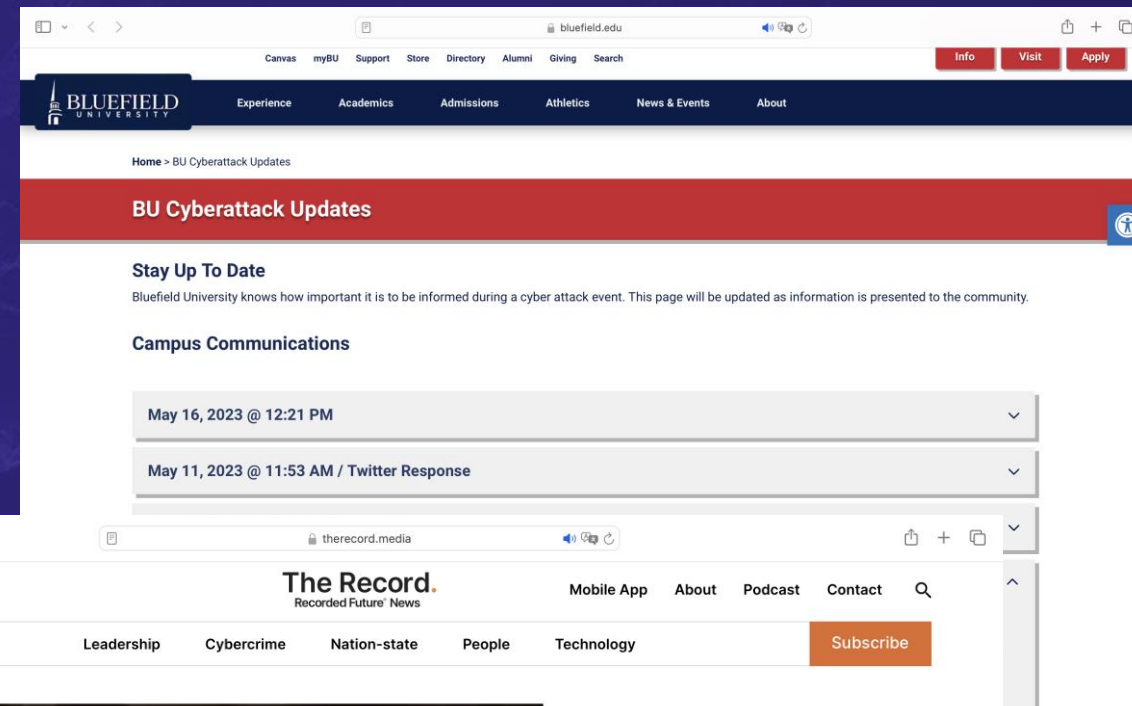
Truman Networks Restored After Cyberattack

Nearly all Truman network services are back online and available after a recent cyberattack.

On the morning of Friday, April 21, Truman ITS found evidence of what appeared to be virus on the University network. In an effort to contain the potential spread, all Truman-issued Windows-based devices and services were powered down and remained inactive, along with the campus network, while ITS responded to the incident. During this time, the University also engaged a firm of outside experts, res cybersecurity resource dispatched to be onsite throughout the week to help resolve the issue.

ITS promptly alerted law enforcement at the time of the incident and it was verified as a form of malware. ITS worked with agents field offices in Kirksville, Kansas City and St. Louis, as well as the Department of Homeland Security, on possible solutions.

On Monday, April 24, ITS conducted preliminary assessments of most primary campus workstations at risk for this particular form of malware and began installing a security patch. By Tuesday, April 25, some network services were brought back online. Additional services will be restored as they are available.



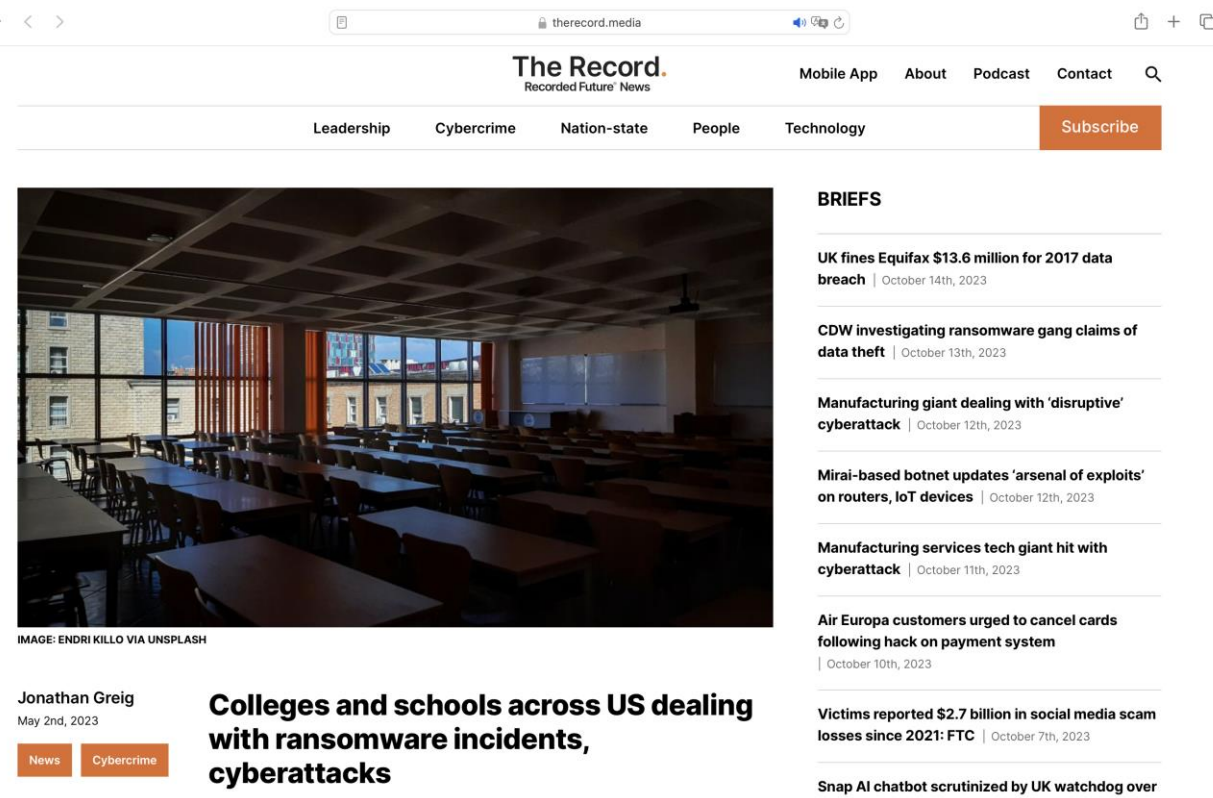
Bluefield University website showing "BU Cyberattack Updates". The page includes a navigation menu, a search bar, and a list of updates. The most recent update is dated May 16, 2023, at 12:21 PM. The page also features a "Stay Up To Date" section and a "Campus Communications" section.

BU Cyberattack Updates

Stay Up To Date
Bluefield University knows how important it is to be informed during a cyber attack event. This page will be updated as information is presented to the community.

Campus Communications

- May 16, 2023 @ 12:21 PM
- May 11, 2023 @ 11:53 AM / Twitter Response



The Record website, a news outlet focused on technology and cybersecurity. The page features a navigation menu, a search bar, and a list of news items. The main article is titled "Colleges and schools across US dealing with ransomware incidents, cyberattacks" by Jonathan Greig, dated May 2nd, 2023. The article includes a large image of a classroom and a list of briefs on the right side.

The Record

Recorded Future News

Colleges and schools across US dealing with ransomware incidents, cyberattacks

Jonathan Greig
May 2nd, 2023

IMAGE: ENDRI KILLO VIA UNSPLASH

BRIEFS

- UK fines Equifax \$13.6 million for 2017 data breach | October 14th, 2023
- CDW investigating ransomware gang claims of data theft | October 13th, 2023
- Manufacturing giant dealing with 'disruptive' cyberattack | October 12th, 2023
- Mirai-based botnet updates 'arsenal of exploits' on routers, IoT devices | October 12th, 2023
- Manufacturing services tech giant hit with cyberattack | October 11th, 2023
- Air Europa customers urged to cancel cards following hack on payment system | October 10th, 2023
- Victims reported \$2.7 billion in social media scam losses since 2021: FTC | October 7th, 2023
- Snap AI chatbot scrutinized by UK watchdog over



Люди, технологии, процессы.

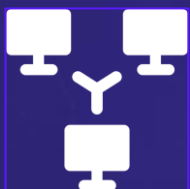
- Повышение кибер-гигиены сотрудников и учащихся
- Использование технологий защиты (XDR, NGFW)
- Документация (инструкции, регламенты, схемы)



Технологии защиты



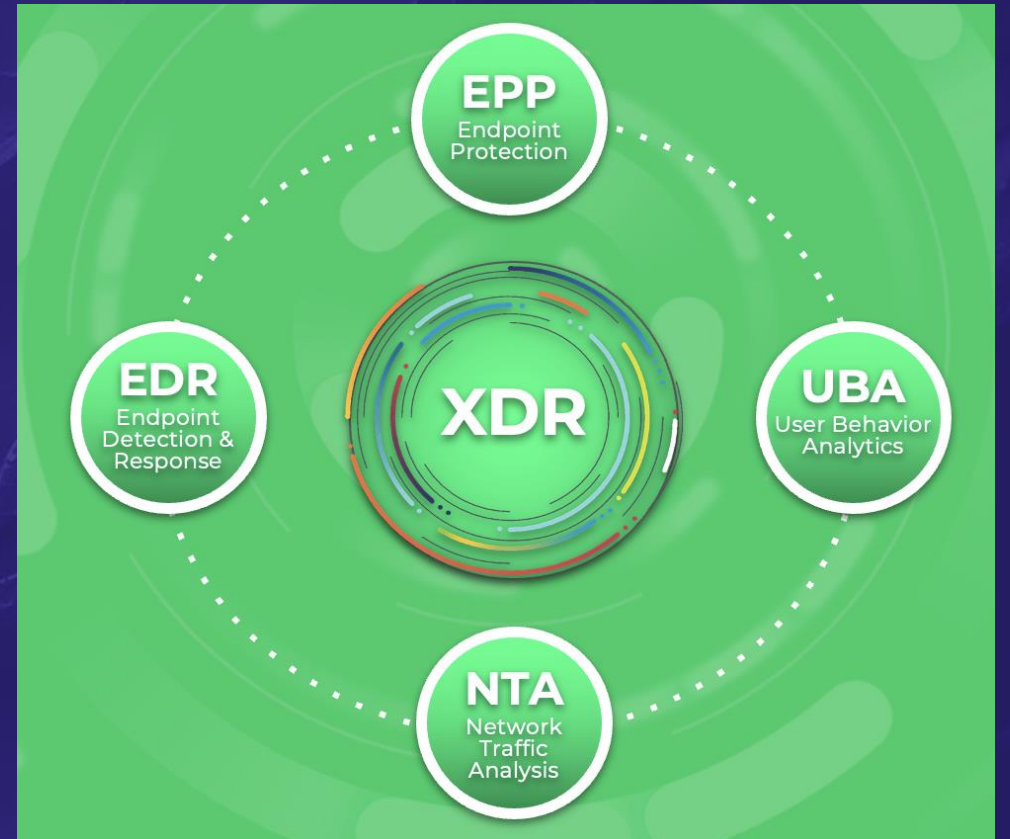
Extended Detection & Response (XDR) – платформа защиты выявляющая и блокирующая целевые атаки и программы-зловреды на любом уровне локальной сети ВУЗа.



Next Generation Firewall (NGFW) – класс продуктов ИБ предназначенный для защиты корпоративных сетей. Детектирует и блокирует вредоносное ПО и аномалии на уровне трафика приложений и зашифрованного трафика HTTPS, SSL и т.д.

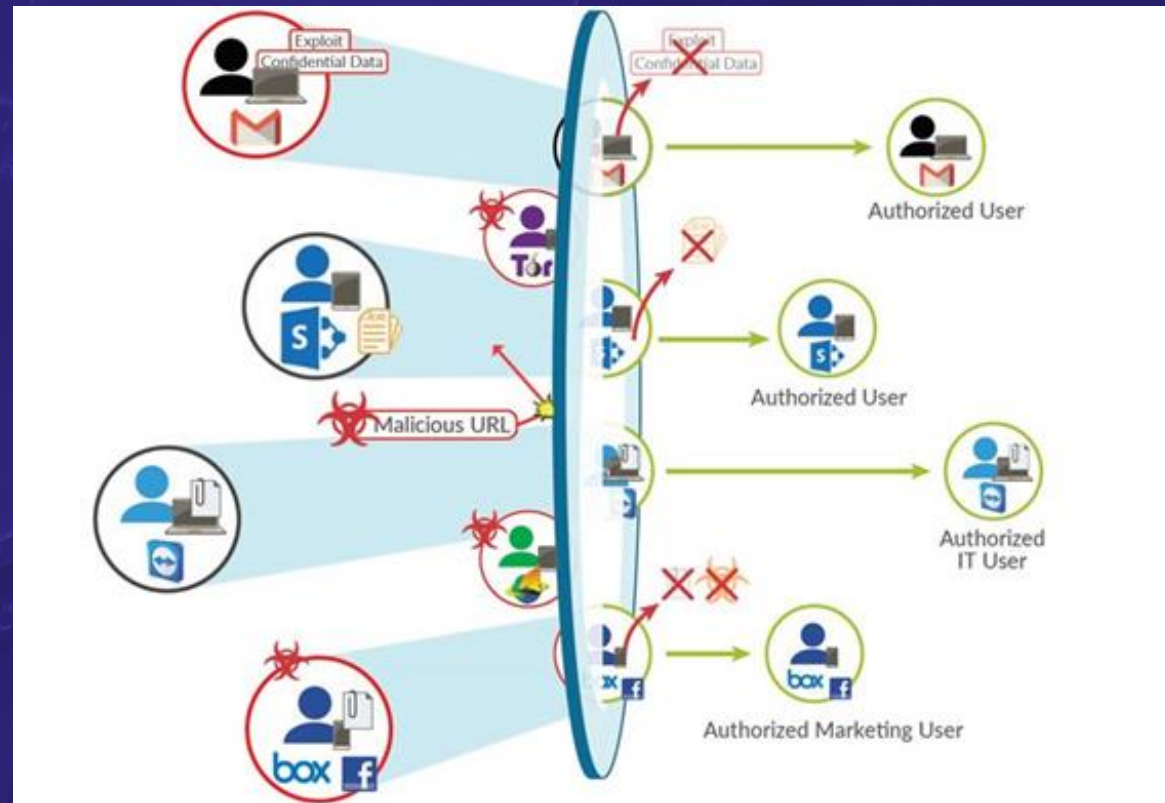
Extended Detection & Response

- Рабочие станции, ноутбуки, мобильные устройства.
- Сервера
- Корпоративная почта
- Виртуальные машины
- Облачные сервисы
- Локальная сеть



Next Generation Firewall (NGFW)

- Защита локальной сети ВУЗ (как в рамках одного корпуса, так и при наличии нескольких корпусов одного ВУЗа).
- Безопасное подключение удалённых пользователей к локальным и облачным сервисам ВУЗ по концепции ZTNA.
- Инспекция трафика на уровне приложений.
- Инспекция внутри трафика HTTPS, SSL.
- Блокировка вредоносного контента, фишинговых ссылок, ПО, элементов целевых атак.
- Разграничение трафика по корпусам ВУЗа по технологии SD-WAN.



«У нас всё есть, значит мы защищены?»

Ручной анализ эффективности ИБ

- Аудит ИБ – проверка документации, актуальности процессов.
- Penetration Test – проверка эффективности средств защиты.

Автоматизированный анализ эффективности ИБ

Breach & Attack Symulation (BAS) – автоматизированная платформа эмуляции кибер-атак.

CAPEX vs OPEX

On prem или MSSP?



Что такое On prem?

- Приобретение в собственность программно-аппаратных продуктов.
- Разовая оплата.
- Нагрузка на текущих ИТ специалистов дополнительных задач в ИБ.
- Обновление программно-аппаратных комплексов раз в 5 лет.



Что такое MSSP?

- Приобретение продуктов ИБ, как услуги.
- Ежемесячная оплата.
- Экспертиза со стороны MSSP-провайдера.
- Всегда актуальная версия продуктов.



В жизни, в танце и в ИБ, главное это партнёр!

- Сертификаты
- Экспертиза
- Опыт в проектах
- Наличие/отсутствие MSSP-модели



На что обращать внимание при выборе технологий

Локальное
присутствие



Саппорт



**Когда же это все
закончится**



Дай Бог мне силы



Alexandr Baitov

TERRITORY MANAGER,
BAKOTECH

Alexandr.Baitov@bakotech.com

+7(771) 170-19-43

bako tech[®]

Рахмет Достар!