AGOR

ПОЛЕЗНИ СЪВЕТИ

Как да сърфираме безопасно в интернет пространството?

Как да предпазим себе си и своите лични данни?

Как да разпознаем различните кибератаки?

Съфинансиран от програма „Еразъм+“ на Европейския съюз

AGOR

С навлизането на цифровите технологии, начинът на общуване между хората претърпява динамични промени. Все по- голяма част от света днес е онлайн! С увеличение на интернет потреблението се увеличава и преноса на данни, което от своя страна, води до повече възможности за работа и свързване между хората от почти всяка точка на света. Това е и основната причина всяка година броят на кибератаките да се увеличава – атакуващите разработват нови, по – сложни методи за получаване на достъп до вашите ресурси, кражба на данни, саботиране на вашия бизнес или изнудване за пари.

Съфинансиран от програма
„Еразъм+“
на Европейския съюз

AGOR

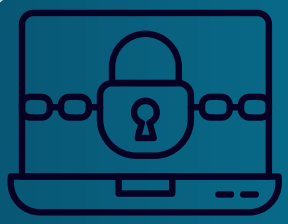
ЩО Е ТО КИБЕРСИГУРНОСТ?

Това са процеси, практики и технологични решения, които помагат да защитите вашата мрежа и критични системи от цифрови атаки.

ЕФЕКТИВНАТА ПРОГРАМА ЗА КИБЕРСИГУРНОСТ ВКЛЮЧВА ХОРА, ПРОЦЕСИ И ТЕХНОЛОГИЧНИ РЕШЕНИЯ, КОИТО ЗАЕДНО НАМАЛЯВАТ РИСКА ОТ ПРЕКЪСВАНЕ НА БИЗНЕСА, ФИНАНСОВИ ЗАГУБИ И ЩЕТИ ЗА РЕПУТАЦИЯТА ОТ АТАКА.

Съфинансиран от програма „Еразъм+“ на Европейския съюз

AGOR



Основни инструменти на киберпрестъпниците

Съфинансиран от програма
„Еразъм+“
на Европейския съюз

AGOR

Злонамерен софтуер

Злонамереният софтуер описва злонамерени приложения или код, които повреждат или прекъсват нормалното използване на устройството в крайните точки. Когато дадено устройство се зарази със злонамерен софтуер, може да се сблъскате с неупълномощен достъп, компрометирани данни или устройството ви да бъде заключено за използване, освен ако не платите откуп.

Хората, които разпространяват злонамерен софтуер са мотивирани за пари ще използват заразени устройства за стартиране на атаки, като например за получаване на банкови идентификационни данни, събиране на лична информация, която може за бъде продавана, продажба на достъп до изчислителни ресурси или изтръгване на платежна информация от жертвите.

Съфинансиран от програма „Еразъм+“ на Европейския съюз

Вътрешни заплахи

Вътрешните заплахи представляват злонамерени действия, извършени от човек, който има достъп до системите и чувствителната информация на една организация.

Такива хора могат да бъдат служители, изпълнители, клиенти и доверени хора с вътрешен достъп, които злоупотребяват с гласуваното им доверие, като по този начин причиняват пробив в защитата на организацията, да откраднат интелектуална собственост, да организират саботаж, както и да причинят загуба на значителни финансови ресурси

В някои случаи тази вреда е непреднамерена, например когато служител случайно публикува чувствителна информация в личен акаунт в облака.

За да бъдат намалени рисковете от вътрешни заплахи е необходимо стриктно управление на достъпа и разработването на политики за сигурност във всяка една организация.

Съфинансиран от програма „Еразъм+“ на Европейския съюз

Фишингът е вид социално инженерство, което използва имейл, текстови съобщения или гласови съобщения, които изглеждат като от реномиран източник, за да убедят хората да им предоставят чувствителна информация или да щракнат върху непозната връзка. Някои фишинг кампании се изпращат до голям брой хора с надеждата, че един от тях ще щракне. Други кампании, наречени насочен фишинг, се фокусират само върху един човек – например престъпник може да се престори, че е търсещ работа, за да подмами служител да изтегли заразена автобиография.

AGOR

Съфинансиран от програма
„Еразъм+“
на Европейския съюз

Напреднала постоянна заплаха (APT)

Това са сред най – страшните видове кибер заплахи. Те се извършват от хакери, предимно с цел финансова печалба и/или политически шпионаж. Чрез APT атаките се установява дълготрайно присъствие и достъп до заразените мрежи, с цел компрометиране и кражба на данни. APT заплахите могат да причинят щети в особено големи размери, като например загуба на интелектуална собственост и присвояване на чувствителна информация, а също и саботаж на големи, ключови организации.

Рансъмуеър

Това е вид малуеър, който може да шифрова цялата или част от информацията на заразения компютър и изнудва потребителя му да плати откуп, за да бъде информацията му дешифрирана. Разпространението на подобен вид вредителски софтуер силно се увеличава след създаването на биткойна и криптовалутата като цяло. По – голяма част от съществуващия рансъмуеър е за операционна система Windows, но се разработват и все повече заплахи за Linux и OS.

AGOR

Социално инженерство

В социалното инженерство нападателите се възползват от доверието на хората, за да ги заблудят да им дадат поверителна информация за акаунта или да изтеглят злонамерен софтуер. При тези атаки измамниците се маскират като известна марка, колега или приятел и използват психологически техники, като например създаване на чувство за спешност, за да накарат хората да правят това, което искат.

„Zero – day “ заплаха

„Zero - day“ уязвимост представлява слабост или недостатък в софтуер, хадуер или фърмуер, която е неизвестна за разработчика или производителя и за която все още няма наличен коригиращ пач или актуализация- Терминът „zero - day“ идва от факта, че разработчикът има нула дни да реагира и да поправи уязвимостта след нейното откриване и публично оповестяване. „Zero - day“ уязвимостите са сериозна заплаха за сигурността, тъй като предоставят на хакерите възможността да експлоатират слабости, преди те да бъдат открити и коригирани. Ефективната защита изисква комбинация от технологии, добри практики и повишена осведоменост.

Съфинансиран от програма „Еразъм+“ на Европейския съюз

AGOR

Как да се предпазим?

Съфинансиран от програма
„Еразъм+“
на Европейския съюз

AGOR

ЗАЩИТЕТЕ ВАШИТЕ ПРОФИЛИ!!

Използвайте силни пароли – използвайте различни комбинации от малки и големи букви, специални знаци и цифри. Желателно е те да бъдат над 10 символа и да са различни за всички ваши акаунти. Използвайте мениджър на пароли и/ или генератор на такива.

Активирайте двуфакторна автентикация (2FA) -така добавяте втори слой защита, като изисква втори начин за потвърждение (SMS код или приложение за автентикация).

Съфинансиран от програма „Еразъм+“ на Европейския съюз

AGOR

ЗАЩИТЕТЕ ВАШИТЕ ПРОФИЛИ!!

- Използвайте VPN – това е технология, която позволява сигурна и криптирана връзка през публична или несигурна мрежа, като интернет. Основната цел на VPN е да защити поверителността и сигурността на данните, предавани предавани между устройството на потребителя и интернет;
- Внимавайте за фишинг атаки - бъдете подозрителни към неочаквани имейли или съобщения, които изискват лична информация; Проверявайте адресите на изпращачите и не отваряйте подозрителни линкове или прикачени файлове;
- Бъдете внимателни с личната информация, която споделяте онлайн – ограничавайте видимостта на профилите си само за приятели и познати;
- Проверявайте настройките за поверителност;
- Ограничете разрешенията на приложенията;

Бъдете информирани!

Съфинансиран от програма „Еразъм+“ на Европейския съюз

AGOR

Мониторинг на мрежовия трафик – Използвайте различни инструменти, за да анализирате мрежовия трафик и да откривате подозрителна активност.

Настройки за сигурността на браузъра – активирайте защитите на браузъра срещу фишинг и злонамерени сайтове. Инсталирайте разширения за сигурност, като блокиране на реклами и защита от тракинг.

ОТКРИВАЙТЕ ЗАПЛАХИТЕ!

Използвайте актуален антивирусен софтуер – изберете съвременна и надеждна антивирусна програма за своите устройства. Сканирайте ги редовно.

Проверка на логовете – редовно преглеждайте логовете на системата и приложенията за необичайни влизания

Съфинансиран от програма „Еразъм+“ на Европейския съюз

AGOR

СПИРАЙТЕ ЗАПЛАХИТЕ!

Изолация на заплахата – ако откриете заразен файл или програма, изолирайте го, за да предотвратите разпространението му.

Обновяване и пачинг – инсталирайте всички налични актуализации и пачове за операционната система и софтуера

Съфинансиран от програма „Еразъм+“ на Европейския съюз

AGOR

СИГНАЛИЗИРАЙТЕ ДИРЕКЦИЯ КИБЕРПРЕСТЪПНОСТ ПРИ ГДБОП-МВР, АКО СТЕ ЖЕРТВА ИЛИ СВИДЕТЕЛ НА КИБЕРПРЕСТЪПЛЕНИЕ.

ИЗПРАТЕТЕ НИ ИМЕЙЛ С ПОДРОБНО ОПИСАНИЕ НА ИНЦИДЕНТА.

ПРИКАЧЕТЕ СКРИЙНШОТ, СНИМКА ИЛИ ЛОГОВЕ. ПОСОЧЕТЕ СВОИТЕ ИМЕНА, АДРЕС И ТЕЛЕФОН.

Подайте сигнал за киберпрестъпление на
имейл report@cybercrime.bg
или на телефон 0885 525 545

Съфинансиран от програма „Еразъм+“ на Европейския съюз