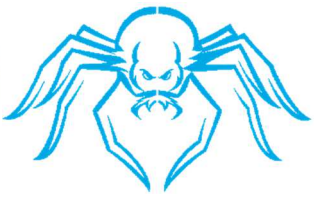


Основни правила за Кибер Сигурност

Автор: Венцислав Върбановски @nu11secur1ty
https://www.nu11secur1ty.com/

##

Бележка: Документа е на български език с цел разпространението и изучаването, на това що е непонятно, за кибер сигурността, на голяма част от българското общество
в редиците на управлвнието на държавата и в голяма част от частния бизнес сектор!

Здравейте приятели, ще започна директно по темата, не съществува понятие като "кибер сигурност", защо?

Причините са три:

1. Конфиденциалност!
- Всяка организация защитава чувствителните си данни, по строго секретен начин.
- Имено поради тази причина няма преподавателско понятие-название за кибер сигурност, а просто елемнтарни основи на кибер сигурността!

2. Политика и закон за защита на интелектуалния труд и чувствителната информация!
- Провеждането на обучения, на всеки три месеца използвайки строго индивидуални методи, за персонала на една организация - компания.
- Изрично се забранява изнасянето на информация, относно въпросните методологии, архитектура, разположение на помещения, сървъри и мрежови координати!
- При неподчинение, изправяне пред Съд и подвеждане под строга отговорност, с отменаме на свобода!

3. Тестове за уязвимости и Контра Атака!
- Строги правила - ОДИТ за спазване, на кибер хигиена от персонала.
- Предварително конфигурирани стационарни компютри - лаптопи, специализирани само за персонала на дадената компания - организация!
- ОГРАНИЧЕНИЕ НА АКАУНТИ и специфичен мрежов достъп на въпросните машини от офисът и личната мрежа, ако са в домашна обстановка! Строго специализиран софтуер за работа, добре къстъмизиран и дебъгнаът фирмен софтуер за защита от евентуална атака от вече работещ служител, за дадената организация – компания! Без осведомяване на въпросния служител, просто предоставяне на машината за работа, и при прихванат опит за злоупотреба от същият този добре къстъмизиран софтуер, прехвърляне към съответните мениджмънт органи и съответно органите на властта!
- Проиграване на всички възможни ситуации при появила се външна и вътрешна атака от неприятел!

- Вземане на превантивни мерки за защита, сведени почти до 99% сигурност и закрила на чувствителната информация!

##

За извършването на горе посочените дейности се наемат ПРОФЕСИОНАЛИСТИ!

Това включва:
- Изграждане на среда:
Системни Администратори ИТ Инфраструктура, Мрежови Администратори ИП Архитекти, Кернел Разработчици, C, C++, Perl, Python, Java и Bash Разработчици, за автоматизиране на работната среда, когато е необходимо!
- Потдръжка:
Дев ОПС инженери, фронт и бекенд Разработчици, Бази Данни Администратори и уеб дизайнери.
- Мониторинг:
Секюрити Анализатори, Секюрити Оперативен Център. Добре подготвени Секюрити Аналитици, готови за адекватно подаване на сигнал за зловредни и застрашаващи сигурността на чувствителната информация кибер атаки срещу компанията!
- Тестове:
Ресърчари, Пенетрешън тестери C, C++, Perl, Python, Java, Bash и други Разработчици.

##

РЕАЛНО: Понятието кибер сигурност съществува просто в разговорния стил на много народи!
Никога не се разкриват специализираните похвати, софтуер и имена на секюрити специалисти наети, за да извършват противодействие срещу кибер атаки и залавянето на кракерите и злонамеремните ИТ специалисти!
СИЕМ или Секюрити Инцидент Ивент Мениджмънт системи за мониторинг.
ВНИМАНИЕ!!! те са просто едно начало, за започване на прояви на отговорност
от срана на менъджерите на определена компания.
Тези ситеми са не ефективни, ако не са подплътени с горе посочените точки и включените към тях условия!

Простете за това че използвам чуждици в тази документация, но ако смятате да се занимавате с дейност като тази, препоръчително е да знаете английски, поне на техническо ниво!

Поздрави и Успех! =)