



## Основни правила за Кибер Сигурност

Автор: Венцислав Върбановски @nullsecurlty

<https://www.nullsecurity.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 управлението на държавата и в голяма част от частния бизнес сектор!

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

Причините са няколко:

### 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 елементарни основи на кибер сигурността!

### 2. Политика и закон за защита на интелектуалния труд и чувствителната информация!

- Тримесечното провеждане, на строго индивидуални обучения на персонала на една организация - компания.
- Изрично се забранява изнасянето на информация, относно въпросните обучения, архитектура, разположение на помещения и сървъри!
- При неподчинение, изправяне пред Съд и подвеждане под строга отговорност, с отменаме с свобода!

### 3. Тестове за уязвимост 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, строго специализиран софтуер за работа, добре къстъмизиран и дебъгнаът фирмен софтуер!
- Проиграване всички възможни ситуации на външна и вътрешна атака от неприятел!

#####

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!

- Поддръжка:

Дев ОПС инженери, фронт и бекенд Разработчици, Бази Данни  
Администратори и уеб дизайнери.

- Мониторинг:

Секюрити Анализатори: Секюрити Оперативен Център - Добре подготвени  
Секюрити Аналитици!

- Тестове:

Ресърчари, Пенетрешън тестери - C, C++, Perl, Python, Java и Bash  
Разработчици.

#####

РЕАЛНО: Понятието кибер сигурност съществува просто в разговорният стил  
на много народи!

Никога не се разкриват специализираните похвати за противодействие  
срещо кибер атаки!

СИЕМ или Секюрити Инцидент Ивен Мениджмънт системите за  
мониторинг, са просто едно начало, за започване на прояви на отговорност  
от страна на мениджерите 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, но ако смятате да се занимавате с  
дейност като тази, препоръчително е да знаете английски!

Поздрави и Успех! =)