



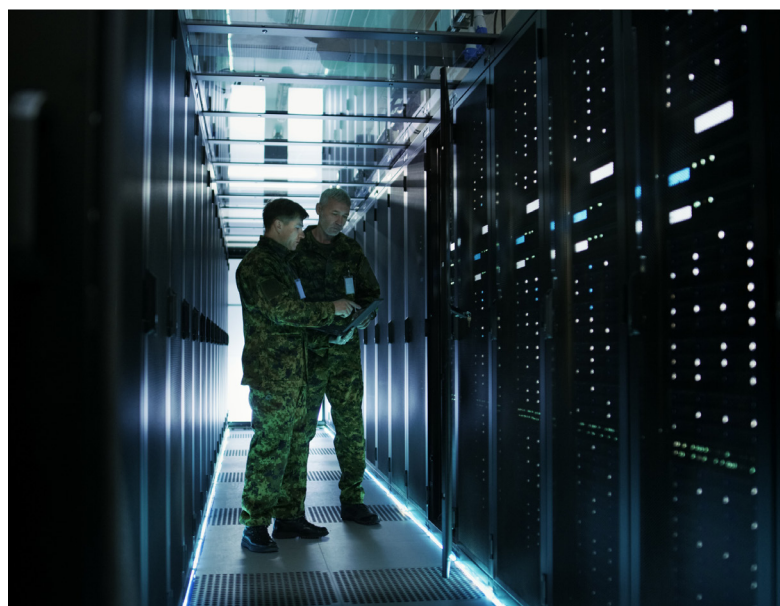
КИБЕРСИГУРНОСТТА – КЛЮЧОВ ЕЛЕМЕНТ ОТ НАЦИОНАЛНАТА СИГУРНОСТ НА ДЪРЖАВАТА

Днес правителствата, организациите и бизнесът по целия свят са изправени всекидневно пред различни кибератаки, при които се правят опити да бъде получен нелегално достъп до чувствителна информация, засягаща важни данни и дори стратегически обекти от национално значение.

На заседанието на Северноатлантическия съвет във Варшава (8-9 юли 2016 г.) се дефинира пети домейн в платформата на НАТО за сигурност и отбрана, където киберсигурността се определя като един от основните приоритети на организацията. Определени са и приоритетните направления като изграждане на колективни способности на Алианса, в това число и включване на киберотбраната в процеса на планиране и на увеличаване на инвестициите на страните членки в тази сфера.

Република България е сред водещите страни, подписали меморандум, в изпълнение на решението от Варшава за обявяването на киберпространството като отделен домейн в НАТО.

В отговор на поетите задължения, през 2016 г. Министерски съвет приема Националната стратегия за киберсигурност „Киберустойчива България 2020“, а в края на миналата година Народното събрание гласува и „Закон за киберсигурност“. В стратегията и закона се отбелязва, че киберсигурността е ключов елемент от националната сигурност на държавата, а киберпространството се дефинира като специфична „виртуална“ територия без физически граници, в която също трябва да бъдат „гарантирани демократичното функциониране на институциите и основните права и свободи на гражданите“.



Набелязани са следните основни цели:

- Установяване и развитие на националната система за киберсигурност и устойчивост
- Мрежова и информационна сигурност
- Защита и устойчивост на дигитално-зависимите, критични инфраструктури
- Подобряване на взаимодействието и споделяне на информация между държава, бизнес и общество
- Засилване противодействието на киберпрестъпността
- Киберотбрана и защита на националната сигурност
- Международно взаимодействие – кибердипломация и оперативно взаимодействие

В изпълнение на тези цели МО, МВР, ДАНС,

ДАЕУ и останалите компетентни органи в областта на киберсигурността следва адекватно и своевременно да развият и придобият способности за киберотбрана и защита като неразделна част от системата за управление на националната сигурност.

КОНТРАКС, съвместно с един от световните лидери с сферата на отбраната и сигурността, General Dynamics Mission Systems, има потенциала да интегрира решения за справяне с технологичните предизвикателства, стоящи пред държава, правителство и общество. Екип от доказали се в практиката експерти оценяват нивото на риск в различни критични инфраструктури и уязвимостите в техните системи за управление и комуникация от кибератаки с различен произход; отбелязват липсата или непълното реализиране и спазване на фирмени и организационни политики и мерки за информационна сигурност, които са предпоставка и улеснение за киберпрестъпниците. Екипът по киберсигурност е обучен да откри-

ва в киберпространството отклонения от определеното ниво на конфиденциалност, интегритет, достъпност, автентичност и отказоустойчивост на информационните ресурси, системи и услуги. Чрез периодични прегледи и оценка на рисковете и заплахите се предоставят предложения за подобряване на мерките за защита въз основа на правни рамки и регулаторни механизми за реализация на стратегията и националните политики.

Съвместно с General Dynamics Mission Systems, КОНТРАКС предлага:

Защита и интеграция на слоевете на киберпространството

Защита в дълбочина

Активни мерки

Предупреждение за заплахи в бъдеще

Автоматизирани процеси на обучение

kontrax.bg

ДНЕС ГОВОРИМ ЗА КИБЕРСИГУРНОСТ



Днес информационните и комуникационни технологии са критично важни, за да бъде осигурен нормалния достъп до жизненонеобходимите за съвременния човек ресурси и услуги като вода, електричество, здравеопазване, транспорт и инфраструктура. Лесното достигане до тези информационни и комуникационни технологии и ниската цена на устройствата и машините за тях, превръщат впечатляващ брой хора в потенциални контрабандисти на информация, а самата информация - в стратегически ресурс.

Повишаването на нивото на киберсигурност е тема, която вълнува цялото ни общество, докато то става все по-зависимо от глобалната информационна и комуникационна инфраструктура. Като всяко общо благо, киберпространството доказано може да се използва като поле за злоупотреби, а това води след себе си нуждата от адекватна защита.

По своята същност киберсигурността е съвкупност от политики и практики, които защитават компютрите, мрежите, програмите или системите от кибератаки, които в комбинация с множество вектори на атака могат да постигнат големи щети.

Всеки, който разчита на дигиталната инфраструктура, без значение къде се намира, би могъл да бъде засегнат. Последствията биха могли да бъдат в широка скала на въздействие – от причиняващи несериозни проблеми до такива, водещи до фатални загуби – материални, финансови, човешки.

Всеки анализ на киберпространството и заплахите за сигурността, не е грижа само на правителства и държавни органи, търговски дружества или частни лица.

Киберсигурността засяга всички, още повече, когато киберпространството е свят малко известен и разбран.

За повечето хора, киберсигурността се свързва с действието и противодействието на „някакви невидими“ атаки.

Въз основа на досегашната практика бихме могли да обобщим, че съществуват атаки (техники за използване на уязвимостите в една система без разрешение за това), разделени до няколко категории:

- Атаки, нарушаващи физическата сигурност
- Софтуерно-базирани атаки
- Социално инженерство
- Атаки, базирани на уеб приложения

- Мрежово-базирани атаки, включително и безжични мрежи
- В много от тези атаки са ангажирани и използвани техники като:
 - **Ransomware** – зловреден софтуер за криптиране на файлове или цели дискове с цел изискване на финансова отплата за тяхното декриптиране
 - **Data manipulation** – процес на изменение на данните в наличните бази от данни с цел достигане на определена информация Rogue software – зловреден софтуер, който се маскира като законен и крайно необходим за сигурността на системата, а в същото време поврежда операционната система, в която се е инсталирал. Целта е прихващане и злоупотреба на чувствителна информация.
 - **Phishing** – най-разпространената имейл-базирана атака, принадлежаща към социалното инженерство и т. н. Според обема, значимостта и разрушителната сила на нанесените щети определяме следните категории кибератаки:
 - **Кибертероризъм** - използване на текущите технологии с разрушителна цел за постигане на идеологическа или политическа идея на терористичните групи. Атакуващите обикновено целят компрометирането на мрежи, компютърни системи и телекомуникационно оборудване.
 - **Кибершпионаж** - атаки, които са извършени за придобиване по незаконен път достъп до секретна информация, съхранявана в цифров вид.
 - **Кибершпионажът** най-често се използва за придобиване на стратегическо, икономическо, политическо или военно предимство и обикновено е насочено към правителства или други организации, които съхраняват поверителни данни.
 - **Кибервойна** - най-често срещаното политически мотивирано оръжие, чрез което се цели проникване в информационните мрежи на други страни и правителства и предизвикането на политически и икономически смущения наред със сериозни щети.

Това са много добре координирани атаки и обикновено се извършват от хакери със стратегически или военни цели, или кибершпионаж.

Като резултат от бързо развиващия се изкуствен интелект и нови технологии, киберпрестъпленията стават все по-организирани и трудни за откриване. Много от устройствата, които използват могат да бъдат манипулирани и трансформирани в кибероръжия, без дори ние да подозираме, а това да доведе до критични, а в някои случаи фатални последици. Колкото повече комуникираме с устройства чрез интернет, водени от идеята за IoT (Internet of Things), толкова повече сме изложени на риск от атаки и позволяваме да се води „кибервойна“ на виртуално бойно поле без изискването за физическа близост.

Предизвикателствата с разрастването на IoT стават повсеместни, а защитата особено необходима. За това крайно наложително е да се следват няколко основни противодействия за смекчаване и избягване на риска от нежелано посегателство:

- Превантивни контроли или мерки, помагачи да се предотвратят заплахи или атаки към открити/ установени уязвимости в комуникационната среда - например добре обмислена и реализирана физическа сигурност – заключване, ограничаване на достъпа или внедрена софтуерна/ хардуерна система за защита от нежелана външна намеса.
- Мерки или контроли за откриване на уязвимости в системата или средата, сред които задължителните за всяка една среда мониторинг на системите, контрол на достъпа, видеонаблюдение.

- Коригиращи контроли, които помагат за смекчаване на последиците от заплахи или атаки с неблагоприятно въздействие. Това са приети и най-вече осъзнати и спазвани конкретни стъпки и политики, приложени за подобряване на физическата и логическа сигурност.

Все пак всеки един от нас е потенциално слабо звено в киберпространството и осъзнаването на този факт е първа, важна крачка в защитата му.

Ако искате да проверите дали вашата компания е в потенциален риск от кибератака, можете да направите своята самооценка още сега, като отговорите на следващите няколко въпроса, които не са изчерпателни, но ще ви насочат къде да бъдете по-внимателни. Ако отговорите на повече от два въпроса с ДА, то вашата компания е в риск.

1. Има ли свободен достъп до Интернет във вашата организация, вкл. WiFi? Да/ Не
2. Има ли вероятност служителите във вашата организация да използват лични средства (компютри, таблети, смарт телефони) за достъп до корпоративна информация, вкл. имейл? Да/ Не
3. Вашите служители имат ли възможност сами да инсталират приложения от интернет пространството? Да/ Не

В случай, че сте установили, че сте в рисковата група, нашите експерти биха могли да ви консултират как да елиминирате възможни заплахи. Свържете се с нас на mail: sales@kontrax.bg като реферирате статията или на телефон 02/960 97 08, където ще получите персонална консултация.

KONTRAX