PROFESSIONAL

Брой 4, година II, юни-септември 2010



ИНДУСТРИАЛНА СИГУРНОСТ

ISSN 1314-0574

Разпространява се безплатно



INFOMEDIA

Инфомедиа ООД/Infomedia ltd.
tel.: (+359 2) 489 1707, mobile: (+359) 887 897 250
Бизнес Център Сердика/Serdika Business Centre
1330, Sofia бул. Иван Гешов 2Е/2Е Ivan Geshov blvd.
www.infomedia.bg

Ikegami

MITSUBISHI ELECTRIC

PELCO

Endura



Кой е най-добрия СОТ? стр. 17



Какво е сейф Промет България стр. 6

СИГУРНОСТ

Конкурентно разузнаване с ограничен бюджет 2

Пликовете за ценни пратки и улики - нови стандарти 4

ЗАЩИТА НА ИНФОРМАЦИЯТА

„Врагът във вашия джоб” 10

Защита на разговорите по GSM 12

Политика за мрежова сигурност 14

Обезпечаване на отдалечен масив от криптирани данни 16

ОХРАНА

Шофирането и проблемите на безопасността 20

НАЦИОНАЛНА СИГУРНОСТ

Понятие за договори свързани с достъп до класифицирана информация 22

БИЗНЕС

За рисковете в бизнеса и тяхното управление 24

Делови етикет и бизнес преговори 26

ЕКСТРЕМНО

Присъединете се към бойното братство 27

Рискове и опасности при екстремните спортове 40

СПЕЦИАЛНИ ЧАСТИ

SWAT
(Special weapons and tactics) 30

ХОБИ

Втора награда не се присъжда-
Как да се научим да стреляме и да улучваме 32

ОРЪЖИЕ

Ловни карабини Томпсън стр. 36





Винтовка ВСС “Винторез” стр. 34

PROFESSIONAL

УВАЖАЕМИ ЧИТАТЕЛИ,

Имаме удоволствието да ви представим новия брой на списание Professional! Първият брой на хартиен носител носи в себе си всички положителни черти и тенденции на досегашните три броя в електронен формат. Ние сме удовлетворени, че тематиката е предизвикала интерес и продължавате да ни четете и по този начин имаме куража да разширим кръгът от потребители, до който изпращаме посланията ни чрез списанието. Водещата тема на този брой е Индустриална сигурност, но в броя ще насочим вашето внимание към управлението на риска, развитието на системите за сигурност, опазването на личната и фирмена информация, екстремните хобита и физическата сигурност. Теми, които напоследък присъстват все по-осезаемо в публичното пространство. Въвеждането и използването на нови технологии, системи и техника пораждат необходимостта от съвременен преглед на личната и корпоративна сигурност. Управлението на риска на всички нива има стратегическо значение за развитието на бизнеса и обществото. Затова в настоящия брой на списанието ще намерите ценни съвети, препоръки и анализи на съществуващите начини за защита от нежелани последствия.

Ще се радваме да получим вашето мнение и препоръки относно темите и списанието или да ни изпратите ваши материали по тематиката коментирана в него.

ПРИЯТНО ЧЕТЕНЕ!

Екипът на Профисек ЕООД

ГЛАВЕН РЕДАКТОР - Николай Цапрев
РЕДАКТОР - Марияна Николова
ИЗДАТЕЛ - ПРОФИСЕК ЕООД

1407 София , ул. Бигла 16А, ет.4
тел./факс: +359 2 962 05 23
e-mail: profisec@abv.bg,
profisec.company@gmail.com
www. profisecbg.com

СНИМКИ - FOTILIA
ТИРАЖ - 3000 копия
ПЕЧАТ - ИНАРТВИЖЪН

Автор: Артур Вайс (Arthur Weiss) - Превод и адаптация: Милен Иванов

КОНКУРЕНТНО РАЗУЗНАВАНЕ С ОГРАНИЧЕН БЮДЖЕТ

Продължение от миналия брой

Събирането на информация при ограничен бюджет винаги започва със събиране на информация от явни източници. Познаването на явните източници и информацията получавана от тях са от голямо значение. Често тя е насочваща и за следващи сфери на изследване и разузнаване. Затова способността да се мисли нестандартно и да се избягват клишетата е ценно качество, което трябва да развиват в себе си всички специалисти по конкурентно разузнаване. Това качество е жизнено необходимо при условия, когато няма достатъчно финансиране. Подобно нестандартно мислене означава способност да се намират необичайни и алтернативни източници на информация. Така например, един от най-добрите безплатни източници на новини за събитията в САЩ не е сайт, разположен в Америка, а уеб сайта на британското издание „UK Financial Times".

Службите за конкурентно разузнаване, които не изпитват недостатъци във финансирането, могат да получат достъп до най-различни инструменти и източници. За нискобюджетните служби голяма част от тези ресурси са недостъпни, а и никой не може да гарантира, че даже в успешна компания няма да съкратят финансирането. Затова специалистите по конкурентно разузнаване трябва постоянно да търсят евтини или напълно безплатни източници. Така например, членството в професионални или търговски асоциации може да осигури достъп до библиотеките на тези асоциации, в това число и до отчети и аналитични статии. Освен това, специалистите по конкурентно разузнаване трябва да се научат професионално да използват Интернет. Когато няма финансиране се налага много неща да се търсят самостоятелно. Това позволява вместване в рамките на ограничения бюджет, но пък губи много време. Професионалните конкурентни разузнавания, които са с ограничени финансови средства, е добре да обърнат внимание на следните възможности в Интернет:

• Различните средства да търсене в Интернет, техните силни и слаби страни (Хубав англоезичен сайт по тази тема — SearchEngineWatch);
• Средства за търсене в новините (за Великобритания това е NewsBot и Excite News);
• Отраслови портали (на тях има линкове към ресурси по конкретния отрасъл). Във Великобритания отраслови портали се търсят с помощта на търсачката LookSmart;
• Тематичните групи новини, дискусионни групи (форуми), тематични кореспонденции. На Запад се откриват с помощта на ресурсите DejaNews, ForumOne и Liszt. Друг добър източник е SCIP discussion forums.

Западните специалисти препоръчват да се направи регистрация и да се ползват следните сайтове:

• FT.com - сайт на изданието „The Financial Times". Интерес за специалиста по конкурентно разузнаване представлява собствената информация на това издание, съдържаща новини от различни отрасли на икономиката и борсова информация. Особено интересна е базата данни „World Reporter", събираща новини от 3000 печатни издания по целия свят. Услугата на FT.com е безплатна, включително и достъпа до базата данни „World Reporter".
• Northern Light е позиционирана като търсачка. Предоставя качествена услуга за търсене и е насочен към бизнес-потребителите, като събира новини и статии от повече от 6400 източника. В базата данни на Northern Light има и анализи за пазарите на акции и маркетингови изследвания. Цената е няколко долара. Има услуга, която известява абоната за появата на нова информация по интересуващата го тема.
• Powerize предлага безплатен достъп до 2400 източника, обхващащи различни отрасли, а с допълнително заплащате отваря достъп до още няколко хиляди ресурса. Освен тона Powerize самостоятелно пуска новини на икономически теми.
• Transium съхранява информация за повече от 300 000 компании по целия свят, което позволява бързо и лесно да се намери информация за всяка от тях.
• Hoover's поддържа малки досиета на компании, включително и на финансови организации и крупни компании от други отрасли. Информацията се предоставя в удобен формат.
• Company Sleuth следи за публикуваната в Интернет информация за американските компании, акциите на които се продават свободно.

Ценен източник са и мрежи от рода на „Facebook", картотеки и бази данни на частни и държавни структури. Всички компетентни специалисти по конкурентно разузнаване трябва не само да са наясно с Интернет, но и да владеят начините за работа с първични източници. Въпреки, че основните принципи на работа са еднакви и за



големите и за малките компании, специалистите в малките са принудени да правят всичко сами. Дори външни консултанти или фирми, занимаващи се с маркетингови изследвания, не могат да помогнат. Необходимо е да се отделя допълнително внимание на следните въпроси:

• Да се внимава, да не се преминат границите на законността и етичността.
• Преди контакт с източник на информация трябва да се планира и подготви срещата.
• Да се планира времето, необходимо за изпълнение на работата - тъй като специалистът работи самостоятелно, той трябва внимателно да прецени своето време, тъй като няма възможност да се обърне за помощ към колега.
• Трябва постоянно да се разширяват деловите контакти. Хубаво е ако специалистът познава лично служителите на своята компания, но това не е достатъчно. Необходимо е да се разширява базата данни с външни контакти - хора, които се ориентират добре в бизнеса, в коя компания работят и т.н. клиенти, доставчици, членове на професионални асоциации, журналисти, които пишат статии за икономически списания, експерти в отрасли и др.
• Необходими са неформални връзки в своя сегмент на пазара. Да се посещават всички изложби и панаири и да се правят запознанства там.
• Познаването на нужните хора трябва да стане втора природа на специалиста по конкурентно разузнаване.
• Да се влезе във всички професионални асоциации, в които може да се направят запознанства с нужните хора и да се получат безплатни списания за членовете на асоциацията.

В статията са дадени няколко идеи за работа на специалистите по конкурентно разузнаване. Те далеч не изчерпват всички възможности. Ако специалистът по конкурентно разузнаване е с ограничен бюджет, той може да компенсира това с креативно мислене, комбинативност и търсене на евтини източници на информация. Парите позволяват да се икономиса време и обратното, липсата им може да се компенсира с допълнителни разходи на време, затова е необходимо да се планира точно. Важно е да бъде ясно кога да се спре събирането на информация. Това е свързано, както със законовите и етични норми, така и с момента, в който разходите за набавяне, превишават ползата от получената информация.

В недостатъчното финансиране по принцип няма нищо лошо. Докато специалистът по конкурентно разузнаване не вдигне телефонната слушалка, не изпрати електронна поща или не се договори за среща с човек, той не може да намери източник, който да е способен да му даде нужната информация. Именно от специалиста, а не от парите в голяма степен зависи резултата. Да, без пари няма да можете да наемете някой, който да ви помогне, но това означава само, че служителят в конкурентното разузнаване, който не е достатъчно финансиран, просто е длъжен да направи много сам. Само така специалистът може да изпълни работата, която му е възложена и да защити интересите на компанията.

ПЛИКОВЕТЕ ЗА ЦЕННИ ПРАТКИ И УЛИКИ – НОВИТЕ СТАНДАРТИ

Знаете ли какво ще се случи, ако поставите улика в обикновен найлонов плик? Най-вероятно тя ще се замърси и един престъпник няма да влезе в затвора. Ами ако банката започне да трупа парите си в хартиени торбички? Най-вероятно друг престъпник ще ги подмени за норматив с фалшификати, а клиентите няма да бъдат особено доволни. Затова криминалисти и банкови служители използват специални пликове, в които трябва да бъдат съхранени и пренасяни ценните пратки или потенциално важните улики. Освен от банките, охранителните фирми и полицията, тези полиетиленови пликове с високо ниво на защита се ползват и в много други сфери – логистиката, земеделието, куриерските услуги и др.

През последните години компаниите във финансовия и логистичния сектор, както и опериращите в сферата на сигурността, стават все по-взискателни към качество качеството на пликовете за пратки. Често освен стойността на пратките е важна и конфиденциалността на пренасяните документи. Поради тази причина тенденциите в производството на този тип изделия са свързани все повече с налагането на високи стандарти за контрол.

„В нашия бизнес е от изключителна важност качеството на услугата – когато става въпрос за сигурност, няма място за компромиси. Именно затова ние работим и с най-добрите в Европа в сферата на опаковъчните продукти за ценни пратки – Debatin“, казва Васко Балабанов, управител във VIP Security. Компанията за услуги за сигурност е доставчик за България на продуктите на немската компания Debatin - най-големият европейски производител на опаковки за логистичния сектор.

Изградените стандарти за производството на пликове за ценни пратки и улики

Контролът на качеството и рутинните тестове на всеки компонент от продуктите се извършват в собствени лаборатории на фирмите-производителки. По този начин се гарантира и запазването на високото качество, което да гарантира сигурността и съответно лоялността на клиентите.

В големите компании като Debatin всеки плик е уникален. Високите стандарти в сектора изискват постоянен контрол и затова всеки артикул има индивидуален номер и баркод. Тези номера се ползват за проследяването на отделните партиди и по този начин гарантират надеждна информация и обратна връзка за стоките. Производителите предлагат дори специфични системи за администриране на номерата и кодовете, което допълнително улеснява клиентите при управлението на техните пратки.

Как да познаем качествения плик за пренасяне на ценности

Благодарение на технологиите, производството на пликове за ценни пратки или доказателства е достигнало високо ниво на сигурност. Как обаче да познаем наистина качествения продукт? Добрите пликовете задължително са направени от силна и устойчива на разкъсване двойна спойка по краищата. Материалът, от който се изработват, е предимно нископлътен полиетилен (LDPE), като в зависимост от нуждите материята може да бъде прозрачна или непрозрачна. Обособени са зони, върху които може да се пише с химикал, както и една или няколко бланки за описание, които могат да бъдат откъснати при нужда. Високите стандарти изискват и всеки плик да има уникален идентификационен номер, който може да бъде придружен и от баркод.

Съществуват няколко различни начина на запечатване на пликовете за пренасяне на ценности или улики. Обикновено производителите ползват т. нар. перманентно запечатване, което е подходящо за пратки на по-ниска стойност. Някои компании като Debatin обаче изработват собствени технологии на запечатване, които са температурно и химически подсигурени. Немският производител е патентовал технолоията Debatape, която представлява залепваща лента с метални нишки.

Промяната в събирането на доказателства в Германия

Само преди по-малко от година немската полиция бе принудена да промени сериозно начина си на работа при събиране на доказателства с наличие на ДНК-проби. Пробивът се случва в малкия германски град Хайлброн, намиращ се на 50 километра северно от Щутгарт. След близо двегодишно разследване местната полиция е уверена, че е по следите на изтънчена престъпничка, отговорна за убийството на полицай в Хайлброн и множество кражби от летни вили. Следователите последователно намират ДНК от заподозряната на няколко сцени на престъпления в цяла Европа.

През март 2009 обаче се оказва, че „виновната“ всъщност работи в компанията, която произвежда памучните тампони за взимане на доказателства от местопрестъплението. Неумишлено лаборантката е оставила своя ДНК по време на опаковането на стерилните



тампони и по този начин е „разпространила“ своя генетичен материал на всяко място на инцидент, където те са ползвани за взимане на доказателства.

На практика този случай дава началото на нова ера в събирането на съдебни доказателства в Германия – специално създадената експертна комисия от микробиолози и следователи препоръча да бъдат многократно завишени стандартите при ползването на приспособления за събиране на доказателства от местопрестъпленията.

Това доведе до създаването на изцяло нови технологии за производството на пликовете за улики. Новите консумативи съдържат перфектна и надеждна защита срещу отваряне от неоторизирани лица – сега всеки подобен опит оставя следи и на практика свежда до нула ефекта от подобно нарушаване на целостта на опаковката.

Не съвсем като на кино

Да управляваш пари е не само привилегия, а и сериозна отговорност. Защото за разлика от филмите, в живота всяко престъпление носи и сериозно наказание. Независимо дали става въпрос за лоша грижа към клиентите от страна на банкер или недобре свършена работа на полицай. За всички, които се отнасят с отговорност към своята работа, решението е едно – те използват пликовете на Debatin.

Промет България ЕООД

КАКВО Е СЕЙФ?

ЗАЩО ИМА РАЗЛИКА МЕЖДУ „ВЗЛОМОУСТОЙЧИВИТЕ” И „ОГНЕУПОРНИТЕ” СЕЙФОВЕ?

Според стандарта, сейфът е устройство с площ не повече от 2 кв. м., предназначено за съхраняване на ценности, документи и носители на информация, устойчиво на взлом. Поради това, всички сейфове са взломоустойчиви, но някои от тях са устойчиви и на въздействието от пожар - те се наричат „огнеупорни”.

Устойчивостта на взлом се определя от броя на единиците на резистентност **Ес**, получени чрез пробиване на касата с **частичен** (проникване през дупка по стандартен шаблон до 300 на 300мм) или **пълен** достъп (проникване в каса през дупка по стандартен шаблон с по-големи размери или отваряне на вратата на минимална широчина 300 мм).

Много често продавачите заблуждават потребителите приписвайки на всички сейфове взломоустойчиви и огнеупорни свойства. В действителност да осигури защита от пожар може само сейф, който е сертифициран и има сертификат за това. Сейфове, притежаващи двата сертификата (за взлом и устойчивост на огън), в действителност са редки и доста скъпи. Освен това осигуряването на взломоустойчивост и устойчивост на огън се постига на практика по напълно противоположни методи, така че основната комбинация, която се среща е от клас I (взлом) и 60 минути (огнеупорност).

Какви други сейфове съществуват?

Най-често те са класифицирани в зависимост от предназначението:

огнеупорни - защита на съдържанието на сейфа от висока температура, но не и от кражба с взлом (професионалист би могъл да отвори такъв сейф за 10-20 минути);

взломоустойчиви - за защита на съдържанието на сейфа от опитите за несанкциониран достъп, не предпазват от пожар;

комбинирани - взломоустойчиви и огнеупорни

вградени – за монтаж (вкопаване) в стена или под, взломоустойчиви, осигуряват и известна защита срещу пожар, тъй като са в стената;

касови- сейфове с клас на взлом 3 и повече, използват се от банки и други финансови институции;

мебелни - обикновено с малък размер за инсталиране в мебели, желателно е да се прикрепят към стена или под;

хотелски - вид мебелни сейфове, оборудвани със специални ключалки за да се улесни работата със сейфа за клиенти на хотели и обслужващия персонал;

оръжейни - за съхраняване на оръжие, оборудвани са със специални държачи и отделения за съхраняване на муниции;

за магнитни носители - за защита на информационни носители - дискети, филми, CD и др. от огън (максимално допустима вътрешна температура при пожар – до 50 ^{O}C - 70 ^{O}C);

депозитни – сейфове за пари, над основния сейф има приемно устройство за пари, в което те се поставят, след затварянето му те се прехвърля автоматично към долното отделение

Трябва ли да се закрепят сейфовете към пода или стената?

Сейфът трябва да бъдат закрепен към пода и/или стената, за да се предотврати възможността за изнасянето му и по-нататъшното отваряне в удобни за крадците условия. Препоръчва се монтажът да се извършва с болтове, които са изработени от твърда стомана и могат да издържат на натоварването на скъсване от 500 кг до 3 тона (дължина от 5 до 30 см и диаметър от 5 до 20 мм).

Застраховат ли застрахователните компании сейфове и тяхното съдържание?

Да, някои европейски застрахователни компании застраховат съдържанието на сейфове или самите сейфове като имущество. В Европа сумата на застраховката зависи от класа на сейфа. Ето ориентировъчние суми за застрахователно покритие за Германия в случай на разбиване на сейфове от различни класове:

Клас [1]	За юридически лица (Евро)	За физически лица (Евро)
1.	40 000	125 000
2 .	100 000	200 000
3 .	200 000	300 000
4 .	300 000	500 000
5 .	500 000	750 000

Какви документи е необходимо да изискате при закупуване на сейф?

Сейфовете са обект на задължително сертифициране. При закупуване на сейф, вие трябва да получите копие от сертификата за съответствие към даден стандарт, в който се посочва класа на защита от взлом и/или пожар. Отсъствието на сертификат може да означава некачествен

1. Клас устойчивост на взлом - (ЕВРО VdS), EN 1143-1



продукт, който не осигурява адекватна защита
На кои организации, издаващи сертификати, можете да се доверите?

Има редица признати сертифициращи центрове на изпитанията, на които може да се вярва. В Европа това са института на застрахователите (Германия, Кьолн), извършващ тестове по стандартите EURO VDS/ EN 1143-1 и EN 1047-1/, Изпитателния център в Брауншвайг (Германия), извършващ тестове по стандартите VdMA. В България изпитанията и сертификацията се провеждат от Техно тест /по БДС EN 1143-1/. Всички сертификати, издадени от производителя или неакредитирани институции или лаборатории, са подвеждащи и са нелегитимни. Обикновено такива се прилагат с цел заблуда на клиента относно потребителските качества на продуктите.

От какво да се ръководим при избора на сейф?

Да знаете отговорите на следните въпроси:
Какво и с каква големина ще съхраняваме в сейфа?
Какво в най-голяма степен би могло да застраши съдържанието на сейфа?
Сертифициран ли е сейфът за устойчивост към взлом или пожар?
Има ли сертификат и отбелязано ли е това от вътрешната страна на вратата на сейфа?
Какъв е обемът и теглото му?
Какъв е типът заключване?
Къде ще се намира?



Има ли гаранция и следгаранционно сервизно обслужване?

Всеки купувач трябва да си представи обема и количеството на подлежащите на съхранение предмети, да осъзнава важността на документите и ценностите, да вземе предвид степента на сигурност на помещението, в което ще бъде инсталиран сейфа, в това число и наличието или липсата на охрана. Също така е необходимо да се оцени най-вероятната опасност (кражба чрез взлом или пожар). Според европейската статистика в девет от десет случая съдържанието на сейф е под заплаха от унищожаване поради пожар и само в един - в резултат от неоторизиран достъп, т.е. кражба. В България, за съжаление, съотношението е в полза на кражбите. Необходимо е да се определи най-подходящия вид на брави: ключова или кодова (с механичен или електронен код).
За оценка на действителното качество на сейфа е много важно да се уверите, че предполагаемите качествени параметри се потвърждават от сертификационните табелки, които са от вътрешната страна на вратата на сейфа. На тези табелки трябва да бъдат посочени: страната на производство, име на организацията, провела сертифицирането, стандарта, по който е сертифициран конкретния сейф.



ПРОМЕТ-БЪЛГАРИЯ” ЕООД
гр. София, р-н Връбница,
с. Мрамор, ул.”Христо Ботев” 28
телефон и факс:02/ 934-98-20, 02/934-98-21, 02/ 998-26-70
prometgroup@mail.bg; www.safe-bg.com

GIGA-DEV.COM
Сайт за компютърна разработка

ЛОВЕН МАГАЗИН
ХЪНТИНГ ГРУП
ВИЖТЕ И
www.gumibus.info
Доставки от
cabelas.com и
basspro.com
195 лв.
Cabela's Gore-tex, Goodyear
195 лв.
195 лв.
120 лв.
170 лв.
75 лв.
165 лв.
Rocky Gore-tex и Vibram
105 лв.
София, бул. “Арсеналски”123
тел. 02/ 480 40 00, 0888/ 486 169

Николай Цапрев

„ВРАГЪТ ВЪВ ВАШИЯ ДЖОБ”

Продължение от миналия брой

От началото на месец март в няколко български сайта вече активно се предлага софтуер или чип за подслушване на GSM. Цените са народни – в порядъка между 400 и 500 лева. Инсталацията и настройката се извършват за около час.

Описаното по горе показва, че световните тенденции в подслушването са приложими в България и нерегламентираното подслушване е все по-достъпно и близо до нас. Тази тема се разглежда в последните два броя на списание PROFESSIONAL. В няколко сайта се появиха компилации на статиите „Врагът във вашия джоб” от брой 2 и 3. Това, както и темата на най-често свалянатa от сайта на Професик ЕООД статия, показват, че въпросът е актуален и вълнува хората.

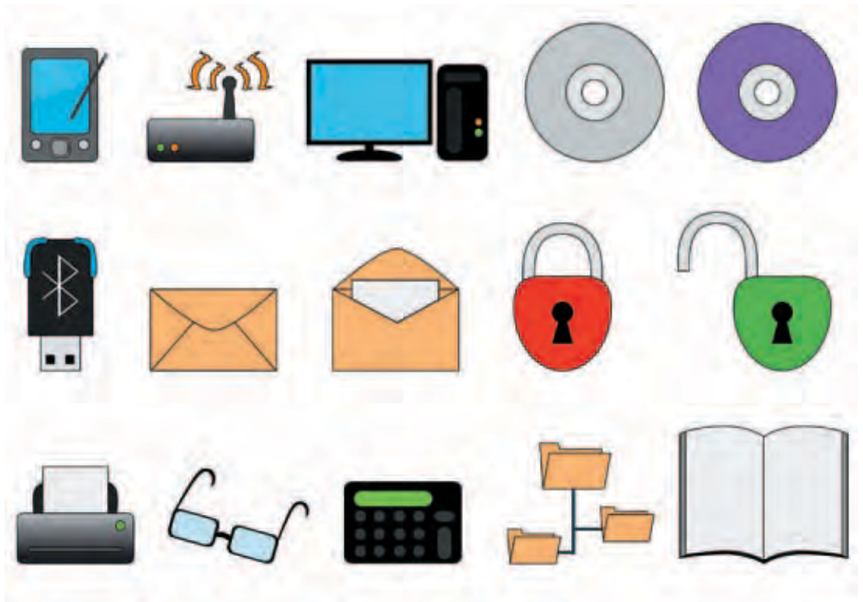
В първите две статии от поредицата „Врагът във вашия джоб” са описани възможностите за подслушване на GSM апарат или подслушване чрез него, използвайки мобилните оператори или шпионски софтуер. Също така са описани възможностите GSM апарата да бъде използван като устройство за несанкционирано получаване на информация, съхранение и пренос на такава.

В тази статия ще разгледаме друг аспект на проблема със сигурността на комуникацията през GSM. Това е прихващането на допълнителните безжични комуникации вградени в мобилните телефони. По точно възможностите за подслушване на телефона и достъп до информацията в него, при работа през комуникационните му портове.

Почти всички мобилни телефони имат възможност за безжична връзка с други телефони, компютри или устройства. Това са Wi-Fi и Bluetooth връзките. И двата типа връзка се активират от ползващия апарата при нужда и не са основен вид комуникация на GSM апарата.

През Wi-Fi обикновено телефона се свързва към безжични точки на интернет. Това може да бъде безжичен рутер на домашната безжична мрежа, но най-често са мрежи със свободен достъп на обществени места като аерогари, музеи, молове, хотели, паркове и други. При връзката с интернет през Wi-Fi телефонът на практика е обикновен компютър, свързан безжично с интернет. Тук възникват два проблема.

Първият проблем е възможността телефона да бъде атакуван през интернет и от него да бъде изтеглена цялата информация, както и да бъде заразен с вирус. Вторият проблем е хакването на безжичната връзка. Влизането в обществени мрежи без парола за достъп улеснява изключително много прихващането на обменяната информация, както от хакери намиращи се в обхвата на дадената Wi-Fi мрежа, така и от системния администратор на интернет провайдъра, осигуряващ интернет за съответната мрежа. И в двата случая е възможно прихващане на обменяната информация, както и достъп до данните и настройките на телефона.



Проблемът се задълбочава и от характера на обменяната информация чрез този тип връзка. Безжичната връзка най-често се ползва за влизане в е-мейл, интернет банкиране, обмяна на файлове, пароли за достъп до сайтове и електронна търговия, разговори по скайп, влизане във фейсбук и други подобни. В по голямата си част това е концентрирана, конфиденциална информация, понякога пряко свързана със сигурността на финансите и политиката за сигурност на ресурсите, до които имате достъп.

С Bluetooth връзката проблемите са аналогични, както при Wi-Fi, с тази разлика, че по-рядко се ползва за влизане в интернет, а по-често за връзка с компютър, принтер, друг телефон и най-вече за разговори през hands free. Сигурността на Bluetooth връзката зависи от настройките на телефона, които сте задали. Ако сте оставили телефона видим за останалите Bluetooth устройства, с разрешение за свободен достъп или парола за сигурност от рода „0000” или „1234”, които са паролите по подразбиране, на практика сте осигурили свободен достъп до вашия телефон за всеки желаещ. Това означава, че човек, намиращ се в радиус до 10 метра от Вас може сравнително безпроблемно да осъществи достъп до вашия телефон, да изтегли цялата ваша информация или да подслушва разговорите Ви в реално време, и за това не се изискват специални устройства, а малко опит, знания и съответен софтуер. Достъпът, макар и по трудно, може да се осъществи, дори и да сте задали правилните настройки за сигурност на връзката, защото по принцип Bluetooth връзката не е особено надеждна. В градска среда радиусът от 10 метра е абсолютно сигурно разстояние, на което е възможно да се случи това. Истината е, че Bluetooth може да бъде подслушван в града от разстояние 200 и повече метра, но за това са необходими устройства, които не се продават масово на пазара. Все пак такива могат да бъдат закупени или сглобени.

Описахме накратко два начина за достъп до вашата комуникация и информация при използването на мобилен телефон. А замисляли ли сте се какво се случва с вашия GSM и информацията в него, когато апаратът е на ремонт. В сервизния център работят хората, които са най-добре запознати с проблемите на хардуера и софтуера и имат достатъчно познания, време и апаратура, за да въздействат върху вашия GSM апарат. На практика апаратът там е най-уязвим. Тогава в него може да се добави всякакво устройство или софтуер и спокойно да се тества дали работи. Ако някой иска да подслушва вашия мобилен телефон, най-добрия вариант за него и най-лош за вас е телефона да попадне в подходящия сервиз при подходящия човек.

След всичко изписано за проблемите на сигурността, свързани с мобилните телефони, всеки уважаващ себе си параноик незабавно би изхвърлил мобилния си телефон. Изхвърлянето на GSM апарата обаче не е решение за масовия потребител. GSM-ът е устройство, навлязло в нашия живот. Ние ставаме все по-зависими от него с всяка нова функция, измислена и внедрена от инженерите. Проблемът е в начина, по който го ползваме. Поради това, че е изключително удобен и с богати възможности, на практика мобилния телефон се превръща в основно средство за комуникация и съхранение на голямо количество данни. Колкото по-голяма част от нашата комуникация минава през него, колкото по-голямо количество информация съхраняваме в паметта му, толкова по-уязвими сме от подслушване, кражба и загуба на информация или други манипулации.

Решение на проблемите със сигурността на информацията при използването на мобилен телефон е възможно. Мерките са комплексни. Свързани са с обучение на потребителите, създаване на определени навици и организация, използване на технически устройства, хардуерни и софтуерни продукти за локализиране и предотвратяване на опити за несанкциониран достъп до информация от външни лица. А това вече е друга и много сериозна тема, която ще разгледаме в други статии.



Професек ЕООД

ЗАЩИТА НА РАЗГОВОРИТЕ ПО GSM

В световен мащаб опазването на личната информация и конфиденциалността е все по-трудно. В тази статия е представено едно добро софтуерно решение на проблема със защитата на разговорите по мобилните телефони.

Private GSM е отлично средство за съхраняването на сигурността на нашите разговори по мобилни телефони Private GSM е софтуер който се инсталира в телефонните апарати с цел защита на конфиденциалността на разговорите и предотвратяване на опитите за подслушване на нашите обаждания от трети лица.

Ако не са защитени, днес всеки може да ги подслушва. Загубата на конфиденциална информация води до загуби в материално и в морално отношение в бизнеса или в личния живот.

Мрежата на мобилните оператори не е сигурна и нашите обаждания лесно могат да бъдат прихванати. Въпреки законовите рамки т.н., **man-in-the-middle (един от основните методи за подслушване)** по данни от чуждестранния и роден печат, е извън контрола на държава и е достъпен на цени под 5000 евро, което е сериозна заплаха за разговорите. Ето защо освен закони за защитата на конфиденциалността на нашите обаждания са необходими и допълнителни инструменти. PrivateGSM е решение с многобройни възможности:

Предимствата на PrivateGSM

-Лесен за употреба

-Можеш да разговаряш с всеки. Специална опция позволява изпращането на PrivateGSM, чрез SMS на други лица, които не са задължени да закупят продукта.

-Гаранция на сигурността. PrivateGSM използва ZRTP, създадено, произведено и гарантирано от Philip R. Zimmermann **www.philzimmermann.com**, един от най-големите световни експерти на тема криптография и сигурност на телекомуникациите.

Private GSM е създаден против опитите за подслушването от трети страни и предлага военна степен на сигурност на мобилните разговори.

Как функционира?

Private GSM е разработен за работа с апарати **Nokia Symbian S60 3°edition**.

-За гарантирано функциониране на продукта се препоръчва използването на един от следните модели на Nokia : *Nokia 5320 XpressMusic ; Nokia 6110 Navigator ; Nokia 6120 classic; Nokia 6210 Navigator; Nokia 6220 classic; Nokia 6650; Nokia E51; Nokia E61i; Nokia E63; Nokia E66; Nokia E71; Nokia E90 Communicator; Nokia N71; Nokia N73; Nokia N78; Nokia N81; Nokia N81 8GB; Nokia N93; Nokia N93i; Nokia N95; Nokia N95 8GB; Nokia N95-3 NAM; Nokia N96; Nokia N96-3* (Моделите се обновяват периодично)

Private GSM използва военно ниво на криптиране AES256 и Diffie-Hellman алгоритъм за размяна на публични ключове. Гласовото съобщение се криптира и предава под формата на алгоритъм, чрез стандартния дата номер (CSD) към получателя, където се извършва обратното превръщане на алгоритъма в гласово съобщение, посредством уникалния код, генериран единствено и само за съответното обаждане. В края на всяко едно обаждане, генерирания ключ автоматично се унищожава. Качеството на гласовото съобщение е същото както при нормално телефонно обаждане.

Стандартния дата номер (CSD) и използването му при работата с Private GSM е условие за коректното функциониране на програмата.При някои от мобилните оператори се изисква допълнително активиране на стандартния дата номер (CSD). При активирането на CSD линията (често наричана и линия данни/факс) мобилният оператор предоставя на абоната допълнителен номер работещ чрез същата SIM карта.

PRIVATEGSM работи като използва стандартния дата номер **CSD (Circuit Switched Data)** на вашия мобилен оператор. Съответно, за работата на Private GSM е необходимо да активирате дата номер.Оператора трябва да ви предостави номер за приемане и предаване на данни. За коректната работа на Private GSM услугата за приемане и предаване на данни (възможност за изпращане и приемане на факс) трябва да бъде активирана и на двете SIM карти.

Как се активира стандартния дата номер (CSD) при различните оператори:

MTel

*Услугата се казва Номер Данни и Факс (получаване и изпращане на факс съобщения)

*Услугата е достъпна само за абонати, и се активира в магазините на Mtel

*Цена на активация 12 лв с ДДС



GLOBUL

Услугата се казва Данни и Факс на Globul, и е достъпна за всички абонати на Globul, както и за тези в роуминг в мрежата на Globul.

Попълва се заявление за “номер Данни и Факс” във всички магазини Globul

Цена на активация 12 лв с ДДС

VIVATEL

В момента не предлага услугата за приемане и предаване на данни и съответно нямат отделни дата номера, но въпреки това при абонаментните планове е активирана CSD линията и Private GSM функционира на територията на България в чужбина и специално в роуминг не винаги гарантира връзка.

За да работи софтуера е необходим мобилен апарат

*Nokia с операционна система Symbian

*Стандартен дата номер CSD

*Свързване с дилър за инсталация на последната актуализирана версия на Private GSM

*Преди да закупите лиценза може да поискате инсталацията на пробна версия с безплатен период 15 дни.

Private GSM позволява да проверите сигурността на вашето обаждане в момента на осъществяване на връзката. На дисплея на двата телефона при осъществена защитена връзка трябва да се появи т.н. **Short Authentication String (SAS)** съставен на базата на две думи от т.н. **“PGP Word List”** списък

При необходимост от спешен разговор с лице не притежаващо софтуер за защита на разговора, проблема може да се реши на момента. Чрез изпращането на SMS можем да поканим трети лица да инсталират “Receive Only” версията на Private GSM и по този начин да разговаряме по сигурен начин с тях. Версията “Receive Only” позволява приемането на сигурни обаждания но е ограничена в изходящите обаждания.

Законова рамка позволяваща употребата на Private GSM

***България е подписала Васенаарската конвенция**

*Според нея всички асиметрични алгоритми за криптиране до 512 bits - не подлежат на контрол.

Конституция на Република България

*Чл. 34. (1) Свободата и тайната на кореспонденцията и на другите съобщения са неприкосновени.

(2) Изключения от това правило се допускат само с разрешение на съдебната власт, когато това се налага за разкриване или предотвратяване на тежки престъпления.

за повече информация - www.profisecbg.com

Румен Дончев

ПОЛИТИКА ЗА МРЕЖОВА СИГУРНОСТ

Новата поредица от статии ще представи основните моменти от стандартите за информационна сигурност, последователността за създаване на политика за сигурност при управление на информационните (автоматизирани и ръчни) системи, интегрираността, наличността и достъпността на информацията във фирмата, корпорацията, дружеството.

Информацията и информационните технологии са критични активи, осигуряващи бизнес целите на организациите. Успехът и развитието на всяка фирма, корпорация или дружество зависят в голяма степен от възможността на информацията и технологиите да осигурят бизнес процесите, да предоставят на ръководството и клиентите навременна и адекватна информация и да осигурят предимство спрямо конкурентите.

Ръководството на дадена фирма, корпорация или дружество следва да разглежда информацията като актив, влияещ върху работата и развитието на организацията и изискващ съответното ниво на защита от неоторизиран достъп и неправомерна употреба. Защитата на информацията е задължение на всички служители на фирмата, като отделни личности и в екип, което е важно за репутацията, ефикасното изпълнение на задачите и осигуряване на финансови успехи. Информацията може да съществува в различни форми – на хартиен, електронен или друг вид носител, под формата на предмет или устройство, в аудио или визуален формат. Може да се отнася до всички дейности на фирмата или до отделни направления.

Анализа на развитието на информационните технологии показва, че най-слабото звено се оказва човека, който със своето познание или непознание може да нанесе вреди на системата. Причините и мотивите за това могат да бъдат най-различни, затова има необходимост от правила, като тяхното прилагане и контролиране са от голямо значение за работоспособността на корпоративната мрежа.

Сигурността на информацията в ИТ се състои в запазването на нейните елементи:

- **конфиденциалност** – информацията се използва само от оторизираните за това лица;
- **цялостност** – информацията е пълна, правилна и измененията не нарушават нейния интегритет;
- **достъпност** – оторизираните лица имат достъп до информацията, когато това е необходимо.
- **Прилагане на принципа – „НЕОБХОДИМО ДА СЕ ЗНАЕ”**. Това означва, че всеки трябва да има достъп само до необходимата за пряката му работа информация. Сужител, който по длъжностна характеристика не работи с компютърна техника не следва да има достъп до информация в електронен вид.

Най-важният елемент на корпоративната мрежа са сървърите, с които се работи, и на които се събира много и разнообразна информация. Пораженията, които могат да се получат варират от чисто физическо унищожаване, до загуба на информация поради изтриване, както и кражба, злоупотреба с информация и манипулиране на същата. Всяко едно от тези поражения може да доведе до икономически загуби на дружеството.

За запазване цялоста, интегритета и конфедициалноста на информацията в европейски и световен мащаб са разработени и се прилагат стандарти за Информационна сигурност - ISO 17799:2005/ISO 27001:2005, БДС ISO/



IEC 17799:2006, Кодекс за добра практика за управление на сигурността на информацията (БДС ISO/IEC 27001:2006, Системи за управление на сигурността на информацията ISMS. Стандартите описват изискванията към сигурността на информацията и технологиите в информационните системи на дружеството или корпорацията.

Стандартът ISO 17799:2005 съдържа препоръки за управление на информационната сигурност. Той покрива различни аспекти на сигурността като:

- планиране на кризисни ситуации;
- физическа сигурност;
- въпроси на сигурността, свързани с персонала;
- контрол на достъпа до информационните системи;
- сигурност при разработка и поддръжка на информационни системи.

ISO 17799:2005 представя най-добрите практики по сигурността, които могат да бъдат приложени във всяка компания, независимо от нейния размер и спецификата на дейността. Стандартът не е обвързан с определена информационна технология. От своя страна стандартът ISO 27001:2005 дефинира изисквания към системи за информационна сигурност.

Изграждането на система за информационна сигурност в съответствие с изискванията на двойката стандарти ISO 17799:2005 / ISO 27001:2005 е един от най-подходящите начини за управление на рисковете, свързани с информацията във всяка една компания.

Системите за управление на информационната сигурност (Information Security management systems - **ISMS**) имат за цел да гарантират конфиденциалността и интегритета на информационните активи на организацията - внедрител, да управляват надеждния достъп до тях и да оптимизират използваните ресурси по съхраняването им.

Доказан в практиката е подходът да се изгради ISMS въз основа на изискванията на Британския стандарт BS 7799-2:2002 (вече е приет като ISO стандарт 27001:2005) и на набора добри практики, заложени в ISO 17799. ISMS, изградени съобразно изискванията на тези два стандарта обхващат основните аспекти на сигурността: оценка и управление на риска; управление на персонала, физическа сигурност; контрол на достъпа; сигурност при избора, закупуването и ползването на софтуер и хардуер; планове и действия в извънредни ситуации и кризи.

ISMS обхваща основните направления в управлението на всяка организация. В основата на изграждането на Системата за управление на информационната сигурност лежат анализа на активите и анализа на риска.

На базата на тези анализи се формира политика по сигурността, която се обявява в публичното пространство. Определят се уязвимите места, потенциалните заплахи и очакваните последствия при “пробиви” в сигурността на информацията. Подбират се съответните защити (controls), които по принцип попадат в 133 отделни групи съобразно вида заплаха, на която противодействат. Изготвя се т.н. “Декларация за приложимост”, в която организацията заявява какъв вид защити е подбрала и какво е приемливото ниво на остатъчния риск.

Корпоративната политика за информационна сигурност се стреми да намери баланс между потребностите, породени от функциите на фирмата (например продуктивност) и изискванията на сигурността. По необходимост документа се фокусира върху принципите и правилата на работа в компютърната среда.

Всички служители от и извън фирмата имат етичното и морално задължение да защитават вътрешната информация, притежавана или съхранявана от същата, както и да поддържат поверителността на тази вътрешна информация.

Информационен ресурс е всяка система от физически и/или логически свързани технически средства, програмни продукти и потребителски данни, осигуряващи информационно един или повече бизнес процеси. Информационният ресурс осигурява събиране, обработка, съхраняване и експортиране на информацията. Информацията е основния обект на дейността на информационния ресурс.



Достъп до информационните ресурси се предоставя на служителите на фирмата с цел изпълняване на възложените им служебни задачи.

Служителите трябва да знаят и приемат, че съдържаната информация в техните работни станции, електронна поща, гласова поща и другите предоставени им фирмени ресурси не може да се счита за частна.

На служителите може да бъде търсена отговорност за извършени от тях дейности, свързани с използването на фирмени информационни ресурси.

Фирмата следва да допуска използването само на надлежно лицензирани и вътрешно разрешени софтуерни продукти (СП) и системи.

Разработване, внедряване, прилагане и контрол на „Корпоративната политика за информационна сигурност” Политиката за информационна сигурност на фирмата се реализира чрез спазването на “Вътрешни правила за използване на компютърната среда”, с които се определят правата и задълженията на персонала по отношение на използването на компютърната й среда.

Вътрешните правила за използването на компютърната среда трябва да гарантират, че са взети всички разумни мерки за предпазване на обработваната информация от загуби, неразрешен достъп или разкриване на служебна тайна.

Политиката за мрежова сигурност включва редица административни, организационни и технически мероприятия. Те се налагат и реализират чрез общите правила и принципи за осигуряване на информационна сигурност в конкретната фирма. Основната цел на вътрешните правила е от една страна да се дефинират правилата за коректното използване на компютърните ресурси, а от друга - да спомогнат за намаляване на риска по отношение на информационната сигурност.

Политиката за мрежова сигурност изисква използване на комбинирани методи за сигурност, а именно организационни, административни и технически мероприятия.

В тази статия разгледахме общите положения и стандарти при създаването на политика за мрежова сигурност, в следващите от поредицата ще разгледаме конкретни мероприятия по прилагането и в организациите.

по материали от Cryptotel, www.cryptotel.net

ОБЕЗПЕЧАВАНЕ НА ОТДАЛЕЧЕН МАСИВ ОТ КРИПТИРАНИ ДАННИ.

Много от нас в ежедневната си работа създават файлове с чувствително съдържание, което биха предпочели да остане само за частните им нужди. Информационната сигурност стана област с бурно развитие през последните години, но някои от нашите навици така и не се промениха. Смятаме, че „крием" файловете си в скрити директории (папки), архиви с пароли или пощенски кутии. Тези подходи ни спасяват от любопитните ни приятели и роднини, но не са никакво препятствие за тренираният специалист. На база опитът, изграден през годините ви предоставяме един синтез на сигурните практики, които ще оставят хакерите и недоброжелателите в неведение.

Тук ще опишем някои от основните механизми за подсигуряване на данните във всяка една форма. Старо правило е да се използва схема „лукова глава", т.е. същинските данни да бъдат обвити от няколко слоя сигурност при работата с тях и локацията им.

Ключова точка около съставянето на сигурна установка е надеждният алгоритъм за криптиране/хеширане на данните.

Основните избори са 2 : PGP публични ключове и AES/Twofish с MD5/SHA-1

PGP е особено сигурен, но само когато се използва с издадени ключове/сертификати, а не с пароли.

AES-128/AES-256 е удачен избор, тъй като е бърз и се счита за неразбиваем в близките 50 години. Ще опишем AES-256 като първоначален алгоритъм за криптиране.

Има 3 вектора, които трябва да подсигурим, за да очакваме надеждност:

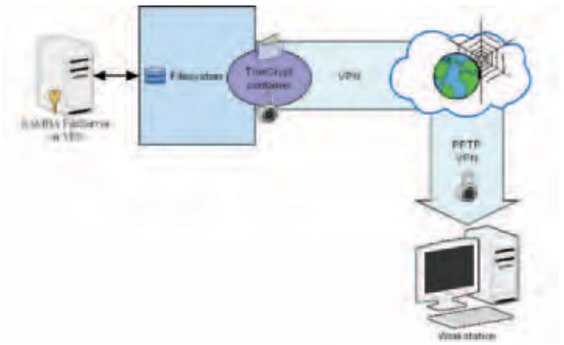
1. Съхранение - Когато говорим за отдалечено съхранение на данни е добре да изберем доставчик с име и история, който да ни осигури надежден uptime. Популярно е използването на виртуални частни сървъри (VPS), като ниските експлоатационни разходи и голямата гъвкавост ги правят сполучлив кандидат за нуждите ни. Цените на най-ниските пакети на пазара започват от около 15 лева на месец, но могат да паднат значително, ако се използват големи чуждестранни доставчици. В описанията си влагаме нулево доверие към евентуален доставчик на хостинг услуги. Не са редки случаите на пробив отвътре или социален инженеринг[1] при такива доставчици. Затова препоръчваме те да се използват само за съхранение на вече криптирани данни.

2. Транспорт - Често е добре да вложите допълнителна сигурност при транспорта на данните от вашите работни станции до сървъра за съхранение. Освен, че дава анонимност (тъй като заявките идват от виртуални адреси в частната мрежа), заявките са криптирани и евентуални инструкции към файловият масив също стават недостъпни за досегателства. Препоръчваме да се ползва PPTP-базиран VPN server (poptop), заради съвместимостта му с windows клиенти без инсталиране на допълнителни приложения. Може да се ползва IPSEC или OpenVPN, но конфигурацията се усложнява.

3. Оперативно криптиране - Тук е най-съществената част при осигуряването на данните. Използвайте софтуер като TrueCrypt (http://truecrypt.org), тъй като сигурността около него е доказана, а ергономията при работа е ненадмината. TrueCrypt (и останалите подобни алтернативи) е крипто драйвър, който използва стандартни команди към файловата система и ги пренасочва към виртуални криптирани „контейнери". С подходяща парола такъв контейнер е невъзможен за декриптиране от недоброжелатели.

Сигурност в движение.

Така подбрани средствата за сигурност осигуряват изключително високо ниво на надеждност при опити за пробив. При правилна конфигурация, имаме 2 набора с



идентификационни данни – за vpn връзката и за truecrypt дяла. При желание може да се въведе и трети слой от сървъра за съхранение на данните – SAMBA username & password.

Недостатъкът на подобна установка е изискването за постоянна връзка към интернет. Но пък преносимостта на услугата е завидна, като нова работна станция може да се конфигурира за по-малко от 5 минути.

Значително удобство е, че можете да монтирате като мрежов диск дялът на файловия сървър и да закачите truecrypt контейнера като дисково устройство. Така ще може да работите с файловете си по начин, по който вече сте свикнали.

Очаквайте детайлни инструкции за създаване на цялата конфигурация. Нашата цел е да предоставим информация на всеки, който не желае да оставя случайностите да ръководят критичните моменти в живота.

1.Ето какво един от легендарните хакери Митник разбира под „социален инженеринг": „Да караш хората да правят неща, които те не биха направили обичайно за непознат, за което освен това ти плащат."

Николай Цапрев

КОЙ Е НАЙ-ДОБРИЯ СОТ?

Често клиенти искат съвет към кой СОТ да се включат, питат кой е най-добрия. Тук ще се опитаме да дадем някои насоки по темата какво означава добър СОТ.

Дейността на СОТ фирмите в България е уредена със „Закон за частната охранителна дейност". Конкретните дейности са записани в следните членове на закона:

Чл. 5. (1) По реда на този закон се извършват следните видове дейности:

1. лична охрана на физически лица;
2. охрана на имуществото на физически или юридически лица;
3. охрана на мероприятия;
4. охрана на ценни пратки и товари;
5. самоохрана.

(2) Дейностите по ал. 1 могат да се осъществяват и чрез технически системи за сигурност и помощни средства.

Чл. 10. Охраната с помощта на технически системи за сигурност е дейност по наблюдение и контрол с технически средства на охраняваните обекти и проверка на получените сигнали.

В случая става дума за дейност, извършвана от търговци, регистрирани по реда на Търговския закон, които са получили лиценз или регистрация по реда на Закона за частната охранителна дейност. Тези търговци (или фирми, както е прието да се наричат) извършват охрана с помощта на технически системи за сигурност. Абревиатурата „СОТ" е придобила гражданственост и идва от съкращението на израза „сигнално-охранителна техника". Много често се виждат надписи „СОД", което би трябвало да означава „сигнално-охранителна дейност". Също така често срещана абревиатура е „АСО". В началото си мислех, че това са фирми от хазартния сектор, но се оказа, че е просто съкращение на израза „Агенция за сигурност и охрана". Например на 29.05.1997 г., Патентното ведомство регистрира стикера и словосъчетанието „СОТ", като запазена марка за услуга (за сигнализация в случай на взлом) на „СОТ – сигнално-охранителна техника" ЕООД, подновена през 2007 г. за следващ десетгодишен период от време – до 09.05.2017 г. Реално в момента правото за използване на абревиатурата СОТ за услуги, свързани със сигнализация в случай на взлом – услуги Клас 37, принадлежи на СОТ ЕООД.

Без значение какви са абревиатурите и имената в България има лицензирани над 1862 фирми, извършващи такава охрана. Нормално е човек да се обърка и да се колебае към кой СОТ да се включи за охрана. Този проблем е най-изразен в големите градове, където обикновено действат над 6-7 утвърдени фирми едновременно, като за София бройката е над 19. Предстои промяна на Закона за частната охранителна дейност. С тази промяна ще се прецизира услугата както и процедурата за лицензиране на лицата имащи право да я извършват.

Нека се опитаме да поставим критерии за добър СОТ. Всъщност СОТ е система от няколко елемента и всеки от тях по отделно влияе на крайния резултат, който трябва да е надеждна охрана на даден обект.. Ако само един от елементите не функционира качествено, крайния резултат е лош.

Първият елемент от системата е изграждането на обекта. Много е важно обектът да е изграден и оборудван с правилната техника, монтирана по подходящ начин. Инженеринговите фирми монтиращи такава техника са над 2500 и в тях работят всякакви „специалисти". Затова при приемане на обектите под охрана служителите на добрия СОТ следва да проверят укрепен ли е обекта и правилно ли е монтирана техниката. Да дадат препоръка ако е необходимо или да откажат поемането на обекта, ако не са изпълнени основни изисквания на сигурността.

Вторият елемент е предаването на сигнали от охранявания обект до мониторинг центъра. Правилно монтираната техника би трябвало да подаде алармен сигнал при нарушение. Добрата техника подава и редица други сигнали относно действията извършвани с нея (включване или изключване на охраната, извършване на ремонт), както и сигнали показващи техническо състояние, например отпаднало захранване, слаби акумулатори, липса на тестов сигнал и други. Тези сигнали се подават периодично и се обработват в мониторинг център. Добрият СОТ гарантира, че тези сигнали ще стигнат до мониторинг центъра. Тоест фирмата има изградена добра мрежа за надежден пренос на сигнала. При липса на добра преносна среда мониторинг центъра няма да получи сигнал или напротив ще получава множество фалшиви сигнали.

Следващ елемент е обработката на получените сигнали. Най-разпространените способи за елиминиране на СОТ са: заглушаване на устройствата, излъчващи алармения сигнал от охранявания обект (радио трансмитер или GSM модул) или прекъсване на линията, по която се предава сигнала (телефонна линия или интернет). Затова важен момент е обработката на тестовите сигнали. В зависимост от използваната апаратура и софтуер, мониторинг центъра очаква да получи тестов сигнал от охранявания обект в

СОТ 161 СПЕЧЕЛЕНО ДОВЕРИЕ

Сигнално - охранителна техника



Централизирана охрана на обекти и реагиране с въоръжени автопатрули

Отдалечено виденаблюдение и мониторинг

Физическа обектова охрана

Персонална и VIP охрана на физически лица

Охрана и транспорт на ценни пратки и съпровождане на товари

Охрана на обществени мероприятия

Съхранение на пари, бижута и ценни предмети в собствен обществен трезор

91 161

0700 10 161

Единен телефон за връзка с дежурните центрове на СОТ161 в цялата страна

www.sot.bg

интервал от 30 минути до 24 часа. Липсата на един тестов сигнал не е повод за тревога и за това повечето софтуери са настроени да подават индикация при липсата на три тестови сигнала. Тоест ако някой заглуши алармата в охранявания обект добрият СОТ ще разбере, че има нещо нередно при липсата на три тестови сигнала или след около час и тридесет минути, а другият след около три денонощия. За съжаления в София има поне две фирми, чиито системи излъчват и обработват тестови сигнали веднъж или два пъти в денонощието, което на практика обезсмисля извършваната от тях охрана. В момента навлизат и по-нови системи за пренос на сигнал и мониторинг. Например изгражданата от СОТ-161 в град София система за мониторинг през GPRS, при която индикацията за техническа нередност или заглушаване се получава на 40-тата секунда. Заглушаването на такава система става безсмислено, защото на 40-тата секунда служителите от мониторинг центъра ще предприемат действия за изясняване на проблема. За решаване на този проблем СОТ 161 има изградена многочестотна инфраструктура за пренос на сигналите, като алармения сигнал може да се предаде на /до/ 7 допълнителни честоти, най често 2-3 back up честоти. 9 радиосистеми и над 22 радиочестоти в София за пренос на сигнали. За важни и рискови обекти се използва дублирана връзка с GPRS комуникация, с тест през 20 сек.

Важен елемент е подготовката на персонала и организацията на работа в мониторинг центъра. Как софтуера и операторите отработват сигналите, получавани от охранявания обект. Преди три години в град София бе разбит и ограбен трезор, охраняван от фирма провеждаща много агресивна рекламна политика в момента. В паметта на компютъра намиращ се в мониторинг центъра на тази фирма бе записано, че в 1 часа на 31.12 срещу 01.01 трезора е отворен с код на служител, имащ право на достъп. Сигналът е получен в мониторинг центъра, но там никой не е обърнал внимание на обстоятелството, че в Новогодишната нощ трезора не работи и не би трябвало да бъде отварян от никого. При добра софтуерна програма, обучение на операторите и създадена организация, този обир е могъл да бъде предотвратен.

Следващ елемент от системата е отработването на сигнала за алармено събитие. Полученият сигнал трябва да бъде забелязан от оператора и предаден на патрула. Тук проблемът е същия, както с получаването на алармен сигнал от обекта в мониторинг центъра. Необходимо е фирмата да има надеждна система за връзка между мониторинг центъра и патрулите. При получаване на сигнал, патрулът следва да реагира. В рамките на 5 минути след задействане на алармата се очаква патрула да посети обекта. В малките градове е лесно това да се случи, но не се получава така в София и големите градове. Как се придвижва патрула, за да стигне на време, как реагира ако в района му има повече от едно алармено събитие едновременно, как се придвижва при големите задръствания? Ако човек се опита да отговори на тези въпроси ще види, че има проблем. Обикновено този проблем се решава с разполагането на множество патрули на ключови места. Ако се загледате в пресечката на Витошка и Патриарх Евтимий в София ще видите поне три патрула на три различни фирми. Мястото е ключово. Патрулите трябва да са достатъчно на брой. За да бъде покрита София е необходимо едновременно да дежурят минимум 33 патрула разположени на ключови места по цялата територия на града. По-малкото от това количество патрули означава невъзможност за своевременна реакция. Не е без значение и какви са превозните средства на патрула. В централна градска част на София в час пик не може да мине нищо друго, освен мотоциклет. В същото време в крайградските части и особено зимно време в полите на Витоша не може да се работи с друго, освен с автомобил с двойно предаване 4х4. В практиката си имах случай, когато при задействане на охранителната система, от фирмата извършваща охраната на обекта се обадиха след 90 минути по телефона, на отговорника на обекта и го попитаха дали има нужда да пращат патрул. Такова действие е абсолютно недопустимо. Някой фирми за СОТ съвместяват едновременно функциите на патрул със сервизен автомобил, логистика и други, поради липса на ресурси, което води до невъзможност за своевременна реакция.

Важно е и поведението на патрула при посещение на обект. Извършването на оглед и анализ на обстановката, както и консултация по телефона с отговорника на обекта, ако същия не е на място, са минимално необходимите действия. При наличие на разбит обект, има случаи, когато охранители довършват започнатото от крадците. За това някой фирми за СОТ имат въведена система за контрол на служителите си и верифициране на събитията.
Отговорността, която фирмата за охрана поема при невъзможност да предотврати инцидент също не е за пренебрегване. Обикновено това е вид застраховка, но се предлагат и други схеми на компенсация.

И накрая всичко опира до цената. Цените са изравнени. Разликата е минимална. Ако разликата е много голяма и в посока към по-ниска цена е редно да се замислим защо. В повечето случаи това е признак за проблем. Не са много тези, които биха могли да подбият пазара с качествена услуга и много по-ниска цена, но дори и това ще е временно. Цената следва да се гледа, след като се изяснят дадените по-горе обстоятелства, влияещи на ефективността на СОТ фирмата. Как да стане това? Ето някои препоръки: чрез разговор с независим специалист, разговор с хора от патрула, официално искане на информация от централата на съответната фирма, преглед на информацията в Интернет и форумите.

Можете и да тествате. Задейства се алармата и се следи реакцията на СОТ компанията. Резултатът си заслужава, дори при евентуалната глоба от 10 евро за неправилно действие.

Ако патрулът се забави повече от 6-7 минути и не получите през това време обаждане или съобщение от мониторинг центъра, по-добре помислете за това с кого и как ще продължите да работите за охраната на дадения обект. Имайте предвид, че фирмите за охрана се отнасят крайно негативно към подобен вид проверки.

Милен Иванов

ШОФИРАНЕТО И ПРОБЛЕМИТЕ НА БЕЗОПАСНОСТТА

Продължение от миналия брой

В статията продължаваме съветите към лицата, извършващи охранителна дейност или към тези, които се притесняват за своята сигурност.

Най-често нападения над охраняваните лица стават при качване и слизане от автомобила. Затова предварително може да се огледа мястото, от което охраняваното лице трябва да се качи в колата или там където трябва да слезе. Ако телохранителят е сам това не винаги може да се прави, но пък при ситуации с неголям риск не е и задължително. Не е желателно да се стои до колата, докато се довършва разговор с някого или се разглеждат забележителности. Необходимо е да се тръгне веднага, без бавене, да се спира колата колкото се може по-близо до изхода. По маршрута за най-опасни се считат първите и последните 50 метра: нападателят може да не знае вашия маршрут, но няма да му е трудно да ви причака до дома или офиса.

Самият автомобил ще бъде атакуван, след като похитителите са изучили подробно маршрута, по който се движи, затова е хубаво да има разработени няколко маршрута и да бъдат използвани без да има система в това. По този начин похитителят няма да може да изчисли точно по кои улици ще мине охраняваното лице. Необходимо е да се избират най-вече оживени и добре осветени трасета. По-добре е да се шофира по-дълго, по хубав път, отколкото да се мине напряко през тъмни и безлюдни пресечки. Да се избягват тесните улички, защото в тях няма място за маневра. Важно е да има готовност по всяко време за престрояване вляво или вдясно, за завои или обръщане в обратна посока. За предпочитане е движението в най-лява лента. В нея скоростта на движение е по-висока и освен това повечето нападения започват с атака на шофьора.

Трудно е да бъде притиснат шофьор към дясната





мантинела или бордюр, като и да бъде заобиколен и настигнат от мотоциклетист от ляво.

Където и да се пътува трябва да се планират минимум два маршрута: основен и резервен. Резервният маршрут трябва да е близо до основния, за да можете да се възползвате от него бързо. И по двата маршрута трябва да сте минали поне веднъж предварително и то в същото време на денонощието, по което ще се използват в охранителен режим. Хубаво е да се отбележат на схемата на маршрута всички проблемни моменти: ремонтни работи, подлези, надлези, задръствания (по кое време?), сложността на отклоненията, ориентири за завиване, разстояния до поделенията на МВР, болници, дежурни аптеки. Трябва да се стремите да сведете до минимум броя на спиранията по маршрута, включително и спиранията на кръстовища - там сте най-уязвими.

Разумно е, когато има възможност, един от телохранителите да изпълнява задълженията на шофьор и постоянно да се намира в автомобила. Обикновено шофьорът е обучен да шофира по правилата и толкова. Телохранителят зад волана трябва да умее доста повече. Никога не бива да се използва автомобила за лични нужди от шофьора и да се возят други хора в него, дори и с разрешение на клиента! “Случаен” пътник може незабелязано да монтира “бръмбар”, мина или да атакува. Не бива да се позволява на клиент в повишен риск сам да отваря, пали, или мести от мястото му автомобил, ако е бил оставен без надзор! Това е длъжен да направи охранителят след щателен оглед. На малка скорост да се провери действието на спирачната система и чак тогава да се позволи на клиента да се качи. Ако „шефа” има желание да шофира сам, нека да има тази възможност, след като телохранителя или шофьора се убеди, че колата е изправна. Желателно е при различните пътувания ако автомобилът е със затъмнени прозорци, охраняваното лице да сменя положението си на задната седалка в ляво или дясно.

Желателно е в автомобила да има колкото се може по-малко страничен шум, например силна музика. Това помага навреме да се чуе сигнал за опасност, технически проблем с автомобила, външен шум /приближаващ мотоциклет/ или клаксон на някой нахалник отзад.

Мобилният телефон винаги трябва да е в готовност, за да се извика помощ. Но ако внезапно пред автомобила изскочи човек с огнестрелно оръжие, телефонът няма да помогне. Подходящо е да се наведете, да натиснете газта и да насочите колата срещу атакуващия. Ако той не успее да отскочи и го ударите, не бива да следвате правилата, които се спазват при пътно транспортно произшествие. Не бива да се спира, за оказване на първа помощ, да се вика “Бърза помощ” или да се чака на мястото КАТ. Трябва да продължете напред. Най-вероятно, похитителят не е сам, и след вас ще последват изстрели. Колкото по-бързо отминете, толкова по-големи са шансовете ви да оцелеете. Даже и автомобилът да е повреден, но все още се движи – натиснете газта! Устойчивостта на много коли е изненадваща. Спомнете си горящия “Мерцедес”, в който се спаси Шеварднадзе!



От друга страна дори и бронирани автомобил няма да издържи дълго време, ако е на място и е подложен на системен обстрел или друг вид атака. Бронираните стъкла обикновено издържат три-четири изстрела в малка площ, след което поддават.

За съжаление описаните мерки за защита не касаят само рисковите личности. Последните две години показаха множество атаки над хора с обикновен бизнес или просто с по-високо благосъстояние. Кой може да бъде заплашен от подготвена атака и какви са признаците за това? Това е тема за друга поредица статии и за специално обучение.

Невин Фети

ПОНЯТИЕ ЗА ДОГОВОРИ, СВЪРЗАНИ С ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

Най-големи проблеми при прилагането на Закона за защита на класифицираната информация (ЗЗКИ) възникват в частта, касаеща индустриалната сигурност. Поради тази причина, както и интерес от страна на бизнес средите, започваме цикъл статии относно приложението на ЗЗКИ при сключване и изпълнение на договори, свързани с достъп до класифицирана информация.

Като вид защита на класифицираната информация, индустриалната сигурност се прилага при сключването или изпълнението на договор, свързан с достъп до класифицирана информация с цел защитата й от нерегламентиран достъп. Приложното поле на индустриалната сигурност е определено максимално общо, като е използвано събирателното понятие за класифицирана информация, което обхваща държавната тайна, служебната тайна и чуждестранната класифицирана информация.

В практиката по прилагане на Закона за защита на класифицираната информация (ЗЗКИ) няма съмнение за необходимостта от коригиращо тълкуване на разпоредбата на чл. 95, ал. 1, от същия закон, аргумент, за което е цялостната уредба на индустриалната сигурност. Тя намира приложение за защита на класифицираната информация, представляваща държавна тайна и не се прилага по отношение на служебната тайна. Това не означава, че при сключване и изпълнение на договор, служебната тайна не се защитава. Защитата й се осъществява с прилагането на т.нар. специални мерки за сигурност. Правилата на индустриалната сигурност могат да се прилагат и спрямо чуждестранна класифицирана информация, но само при условие, че международният договор, по силата на който информацията е предоставена, допуска това. Ако в международния договор не са предвидени специални правила, се прилага законодателството на държавата - източник на информацията.

Законосъобразното приложение на индустриалната сигурност зависи не само от прецизното определяне на видовете класифицираната информация, за защитата на които се използва тази специфична система от мерки. Важно е да се уеднакви смисълът, който се влага в понятието „договор, свързан с достъп до класифицирана информация" или още „договор в областта на индустриалната сигурност", тъй като за тях по правило се прилагат мерките по индустриална сигурност. Употребата на тези две понятия е много по-коректна от израза „класифициран договор", който се използва в почти всички международни споразумения за обмен и взаимна защита на класифицираната информация, сключени между Република България с други държави или международни организации[1] . С несъществени различия в дефинициите, то е определено като договор между двама или повече контрагенти, който съдържа или предполага достъп до класифицирана информация. Проблемът може да се породи от буквалното разбиране на понятието „класифициран договор", единствено като договор на материалния носител, на който е поставен гриф за сигурност. Това значително би стеснило случаите, в които трябва да се прилага индустриалната сигурност и би създало предпоставки за нерегламентиран достъп до класифицирана информация.

Договорите с достъп до класифицирана информация могат да се определят като договори, чийто предмет или изпълнение налага достъп до държавна тайна. Под достъп се разбира не само узнаването на класифицирана информация, но и дейностите по създаване, съхраняване, размножаване, изпращане, получаване, приемане и др. на класифицирана информация, при които се създават условия за узнаването й от други лица.

Конкретните случаи, в които при сключването или изпълнението на договора се налага достъп до държавна тайна, могат да бъдат най-различни. На първо място това са случаите, когато предметът на договора, разбиран като благото, към което този договор е насочен, представлява държавна тайна. Такива например ще бъдат договорите за проектиране, изграждане, снабдяване с оборудване и функциониране на телекомуникационни системи за пренасяне на държавна тайна за нуждите на въоръжените сили, службите за сигурност или организациите по обезпечаване на тези системи, за които е направена преценка, че нерегламентираният достъп може да застраши или увреди националната сигурност. Тези дейности попадат в раздел II, т. 15 от Списъка на категориите информация, подлежаща на класификация като държавна тайна, и при наличие на преценката за съответните заплахи или вреди за националната сигурност, защитата при възлагането им трябва да се проведе по правилата на индустриалната сигурност. Доколкото самият предмет на договора е класифицирана информация, неговото закрепване в определена форма ще наложи създаване на документ, съдържащ класифицирана информация.

Възможно е предметът на договора да не съдържа категории информация, попадащи в списъка на държавната тайна (Приложение № 1 към чл. 25 от ЗЗКИ), но изпълнението на договора да налага достъп до такава информация. Така например мястото на изпълнение на договора може да бъде класифицирана информация, ако дейностите се осъществяват в режимни поделения и обекти по смисъла на чл. 162 от ППЗЗКИ. Доколкото място-изпълнението е включено в текста на договора, това ще наложи не само приложението на мерките по индустриална сигурност, но и класифицирането на текста на договора.

Достъп до класифицирана информация може да се налага не при конкретните дейности по доставяне на дължимия резултат, а при гаранционното обслужване, което изпълнителят се е задължил да предостави. Такава хипотеза може да възникне при проектирането, изграждането и поддръжката на автоматизирани информационни мрежи, в които се създава, съхранява, обработва и предоставя класифицирана информация.

В т. 9 от Задължителните указания за прилагането на принципите и мерките в областта на индустриалната сигурност, издадени от Държавната комисия по сигурността на информацията (решение по протокол № 82 от 19.12.2003 г., изм. с Решение на ДКСИ № 48-I от 04.09.2007 г., изм. и доп. с Решение на ДКСИ № 14-I/24.02.09 г.), се допуска определяне като договор в областта на индустриалната сигурност на договори, чието изпълнение "би могло да наложи достъп до държавна тайна". С тази условна формулировка би могло да се стигне до прилагане на мерките по индустриална сигурност, без да е категорично установена необходимостта от достъп до класифицирана информация. Прилагането на мерките по индустриална сигурност спрямо договори, при които няма достъп до класифицирана информация, създава същия проблем, който възниква при незаконосъобразното класифициране на информацията - предоставя се защита, която правният ред не допуска. Ако липсва класифицирана информация при сключване или изпълнение на договора, прилагането на индустриалната сигурност ще бъде безпредметно, а въведените с нея ограничения ще бъдат лишени от основание. Не бива да се изключва възможността това да има негативен ефект върху система за защита на класифицираната информация, като урони доверието в ефикасността на нейните правила.

За да не бъде произволно приложението на индустриалната сигурност, трябва да бъде преградена възможността тя да се прилага спрямо договори, чието изпълнение би могло да наложи достъп до държавна тайна, без тази възможност да бъде надлежно обоснована. Преразглеждането на установеното в т. 9 от Задължителните указания на ДКСИ понятие за договори в областта на индустриалната сигурност би имало за ефект оптимизирането на установените правила.

Определянето на договорите в областта на индустриалната сигурност поставя важният въпрос за органа, в чиято компетентност е тази преценка. В ЗЗКИ не се съдържа отговор на този въпрос, но Правилникът за прилагане на ЗЗКИ предвижда, че организационната единица-възложител определя предмета на задачата и нейното ниво на класификация преди започване на процедурите по водене на преговори и определяне на изпълнител. Следователно преценката е на бъдещия възложител по договора, което изрично е установено и с чл. 4 от Наредбата за общите изисквания за гарантиране на индустриалната сигурност. Тя се съдържа в нарочен акт, т.нар. схема за класификация, която е част от подготвителните действия по определяне на изпълнител



1. Виж споразуменията с Украйна, Грузия, Италия, Норвегия, Швеция, Гърция, Естония, Латвия, Литва, Македония, Полша, Румъния, Франция, Испания, Словакия, Чехия, Великобритания и Северна Ирландия, Финландия, Хърватия, Албания, Австрия, Португалия.

Димитър Заяков

ЗА РИСКОВЕТЕ В БИЗНЕСА И ТЯХНОТО УПРАВЛЕНИЕ

Когато говорим за рискове в бизнеса и начините за тяхното управление е справедливо да кажем, че по темата има публикувани не малко материали от български и чуждестранни специалисти. Източниците на подобна информация са най-различни – учебници, списания, ръководства и други печатни издания, интернет, закони, наредби и правилници на различни държавни институции и др. В повечето от тях се дава определение на понятието риск, прави се анализ на видовете рискове и се предлагат механизми за тяхното управление или избягване. В тази статия, с цел да не натоварваме читателите с популярна информация, ще се опитаме да направим нещо различно. Ще покажем къде има пропуски в разбирането на понятието риск и къде в управлението на рискове съществуват проблеми, които все още не са намерили адекватно решение. Разбира се, веднага ще направим уговорката, че тук споделяме своето виждане претенции за изчерпателност. По този начин се надяваме да поставим началото на дискусия, в която да достигнем повече яснота по темата.

Състояние на управлението на рискове в България и опит в осъществяването на тази дейност.

Ако направим една анкета между мениджърите от различни нива в България по въпроса „Знаете ли какво е риск мениджмънт и прилагате ли го във Вашата фирма", вероятно ще получим почти сто процентов положителен отговор. Разликата ще бъде в детайлите. И това е разбираемо, защото в последно време за риск и неговото управление се говори активно, провеждат се семинари, обучения т.е. модата на темата е дошла. Различия в детайлите ще има, защото в зависимост от предмета на дейност на организацията и нейната структура е достигнато различно ниво на управленска култура по темата. Най-богат опит в управлението на рискове в недържавната сфера у нас вероятно има в банковото дело и в застрахователния сектор. Там дейността и резултатите в значителна степен зависят от оценката на рисковете и прилагането на системи и механизми за тяхното изследване и анализиране е със сериозна предистория.

В резултат на прилагането на нормативни изисквания, създадени от държавата в сферата на безопасността на труда (например наредба № 5 от 1999 г. на Министерството на труда и социалната политика и на Министерството на здравеопазването) в почти всички, а вероятно и във всички фирми в страната се създадоха, чрез добре известния принцип „копи-пейст", т.н. програми за оценяване на риска, които създадоха за голяма част от мениджърите впечатлението, че проблемите с управлението на риска са решени.

Компаниите, които се занимават с инвестиционна дейност също имат определена практика за оценка на инвестиционния риск, която в значителна степен се доближава до методите на управление на риска, прилагани в банковата сфера.

Успешното, през последните години, развитие на частната охранителна дейност също допринесе значително за решаване на редица проблеми с управлението на рискове, свързани преди всичко с контрола на достъп, охраната и опазването на активите на компаниите, а в някои случаи и с прилагането на модели и механизми за повишаване на информационната сигурност.
За повишаването на сигурността на не малка част от фирмите в страната в последните години беше постигнат и ръст в управлението на рисковете, свързани с човешкия фактор.
В резюме ще отбележим, че бизнесът в България има понятие за една част от рисковете, които го заплашват, а също има изградени навици за управление на някои от тях.

Пропуски в разбирането на понятието риск.

В разбирането на понятието риск и значението на управлението му за икономическата стабилност на фирмите съществуват пропуски, които са в резултат на следните причини:
- липсата на достатъчно ресурс във фирмата за организиране и провеждане на правилно и пълноценно управление на рисковете, които съществуват за нея. Това е една от най-често изтъкваните причини от мениджърите. Тези, които управляват малки и средни предприятия или микропредприятия обикновено споделят, че не са в състояние да отделят финансов и човешки ресурс за изследване, анализ и оценка на риска. Този аргумент се изтъква и от управителите на по-големи фирми. Оказва се, че в повечето случаи те не могат да формулират конкретно и ясно кои са рисковете за тях и как си представят управлението им. Всъщност всяка една фирма, независимо от броя на служителите в нея и финансовите и резултати, може и трябва да прави анализ и оценка на рисковете, които съществуват за нея. Обикновено изразходвания за целта ресурс е пропорционален на възможностите на фирмата. Но непознаването на материята е много по-лесно да бъде преодоляно със самоубеждаването, че „бедите нас не ни засягат";
- липсата на взаимодействие между отделните звена по веригата за анализ и оценка на риска за фирмата. В някои от добре развитите в административно отношение компании в България съществуват отлично или поне добре работещи звена за управление на различните елементи на организацията. Финансово-счетоводните отдели или дирекции, отделите „Човешки ресурси", „Логистика", „Сигурност", „Правен", „Маркетингов" и др. обикновено са съставени от добре подготвени специалисти в тяхната област. Всеки отдел или дирекция провежда мероприятия по анализ и оценка на риска в своето направление. Липсата на взаимодействие по вертикала между тези звена води до невъзможност да бъдат констатирани и предотвратени рискове, които съществуват именно по тази вертикала. Представете си случай, в който „Човешки ресурси" са допуснали назначаването на човек в „Маркетинг", без да направят справка във взаимодействие със „Сигурност", дали този човек не е работил в конкурентна фирма;
- липсата на анализ и оценка на външната за фирмата бизнес среда. Много често такъв анализ и оценка се подценяват, като вниманието на мениджърите е основно ангажирано с вътрешните за фирмата проблеми. Разбира се, има фирми, в които се прави анализ и оценка на външната среда, но той в повечето случаи е фокусиран само в направления, в които са преките интереси на фирмата. По този начин се пропуска възможността да бъдат констатирани и овладени процеси, които оказват индиректно влияние върху икономическата стабилност на фирмата;
- липсата на желание във висшия мениджмънт на компанията да се приложат ефективни механизми за управление на рисковете. Има компании, в които е приложена твърде централизирана форма на управление, при която решенията се взимат от един или много ограничен кръг от хора. В някои от тях висшите мениджъри имат много добра грамотност по управление на рисковете, но поради редица причини от субективен характер, не предприемат действия в тази посока или допускат извършването на такива дейности само до определено ниво.

Проблеми в управлението на рискове, които не са намерили ефективно или адекватно решение.

В състояние ли е всяка една фирма, независимо от ресурсите, с които разполага, да извършва анализ и оценка на риска за своята дейност. Отговорът на този въпрос е категоричен – да. В такъв случай не решаването на проблема е свързано преди всичко с промяна в разбирането на мениджъра за същността на риск мениджмънта и за натрупването на определен минимум от познания за технологиите за осъществяването на този процес. За да се постигне тази промяна в компетентността на мениджърите на частни компании (правя тази забележка, защото в повечето случаи в държавните предприятия и административни структури се извършва редовно обучение на ръководителите от различни нива по управление на рискове) е необходимо в началото те да възприемат една проста истина. А тя е, че управлението на риск е свързано с поемането на адекватна отговорност за икономическата сигурност на фирмата, а в частния бизнес тази отговорност е на всеки отговорен за неговото управление. С други думи, държавата не може да носи пряка отговорност и съответно да организира и гарантира сигурността на компанията. Това е работа на мениджърите. Следователно те са тези, които трябва да са подготвени да формулират общата концепция за заплахите, които съществуват за икономическата сигурност на тяхната фирма.

От тук произлиза и вторият нерешен проблем за голяма част от фирмите, особено попадащите в групата „Малки, средни и микро предприятия" (МСМ), а именно определянето на необходимия ресурс, човешки и финансов, за осъществяване на такава дейност. За тази група предприятия проблемът е решим с използването на услугите на консултанти по управление на рискове. Обективно погледнато тази група предприятия трудно биха могли да обосноват икономическата целесъобразност на поддържането на собствено звено за риск мениджмънт. В повечето случаи много по-ефективно и полезно за тях би било първоначалното консултиране на проблема с компетентни експерти и след това периодичното извършване на одит на фирмата им по въпросите на риска. Справедливо е да се отбележи, че специализираните консултантски компании за управление на риск имат значително по-голям ресурс за извършване на тази дейност и себестойността на тяхната услуга в общия смисъл е по-ниска от собствените разходи, които би направило едно МСМ предприятие. В случая не поставяме за обсъждане въпроса дали изобщо трябва да се поемат такива разходи, защото международния опит показва, че инвестициите в управление на риска, които повишават икономическата сигурност на една фирма са около четири пъти по-малки от разходите, които същата фирма би направила за покриване на щетите от неоценен риск.

Друг проблем, който се наблюдава в управлението на рискове, не само в България, е допускането на компромиси в изграждането на системата за управление на рискове на компанията. В не малко фирми, които са изградили системи за контрол на достъпа и защита на материалните активи чрез мониторингови инсталации (обикновено са известни като СОТ – системи) се счита, че по този начин е решен въпроса със сигурността. Това, разбира се е вярно в известна степен, но не съвсем. Съществуват още редица фактори, от вътрешната и външната среда на фирмата, които оказват, в много случаи невидимо, но пряко влияние върху нейната сигурност. Тези фактори не могат да се изследват с технически средства и тяхното изучаване не е епизодичен процес, а е дейност, която трябва да се осъществява непрекъснато.

Тук достигаме и до един от следващите проблеми - събирането и анализа на информация за външната и вътрешната среда.
Тази дейност в най-общия смисъл на понятието се нарича конкурентно разузнаване. Използват се и други термини, бизнес, делово, аналитично или стратегическо разузнаване. Все още в много фирми, когато се спомене думата „разузнаване" и мениджърите настръхват. Започват да ни гледат с подозрение. Тази реакция към момента е нормална, но излишна. Считам, че е нормална, защото за съжаление у нас през последните години медиите нагнетиха в обществото отрицателно отношение към термина, който много хора свързват с досиета, политика, служби и какво ли още не. В съвременния бизнес свят, обаче, конкурентното разузнаване е прагматична и изключително необходима за развитието на бизнеса дейност. Тя обхваща различни групи от експерти, занимаващи се изследване на пазари, на социалните характеристики на обществото, с динамиката на политическите, демографските, културните и още много други процеси, които оказват пряко и косвено влияние върху бизнес средата. Тази дейност има своя теория и се осъществява по строго научно обосновани механизми. За нейното оптимизиране са създадени и активно се използват редица технически и високо технологични продукти, които позволяват събирането, съхраняването и анализирането на огромни потоци от информация, на базата на което се извършва анализа на бизнес средата.
И тук е мястото да посочим още един проблем, а именно, че тези продукти като цяло не са намерили своето масово приложение в бизнеса. Използват се в строго специализирани дейности, като банковото дело, застраховането, финансите, от части в маркетологията.

Управлението на рискове е изключително важен за сигурността на бизнеса процес. Правилното разбиране за неговата същност и усвояването на методите за неговото осъществяване от страна на мениджърите ще доведе до значително повишаване на защитеността на фирмите, независимо от предмета на тяхната дейност, финансовите им възможности или човешкия им потенциал.

Екип Профисек ЕООД

ДЕЛОВИ ЕТИКЕТ И БИЗНЕС ПРЕГОВОРИ

Продължение от миналия брой

Продължителността на преговорите е различна за представителите на различни култури. Американците, например са нетърпеливи, искат деловото общуване да е възможно най-кратко и преговорите да отнемат минимално количество от време. Участниците в преговорите обикновено правят най-големи отстъпки малко преди края на определения за това срок. Чувството за срочност ги поставя в неизгодно положение в сравнение с партньори, които бързат по-малко.

Участниците в преговорите следва да приемат поканите за закуски, вечери, приеми, церемонии и разходки като възможност за изграждане на лични взаимоотношения и като ключов аспект в процеса на преговори.

По време на преговорите се дава приоритет на проблема. Обръщането на особено внимание на личността на партньора може да бъде възприето като признак на слабост и липса на делови аргументи. Информацията за него, получена по време на подготовката, подсказва в каква окраска да се води диалога. Ако кариерата му е "инженерна", то за него най-интересни и важни ще бъдат техническите аспекти. Ако има кариера на "производственик", тогава ще го привлекат детайлите за реалното изпълнение на проекта. За ръководител "общественик" най-важен ще бъде "човешкия" фактор.

По принцип преговорите се водят от ръководителите на делегациите. Останалите се включват в беседата само при покана от своя лидер. Ако искат да се изкажат е необходимо да поискат разрешение. Ако този ред не се спазва преговорите се дезорганизират. В това има и сериозен психологически елемент. Информацията, изхождаща от лица с по-висок статус се възприема като по-достоверна и значима и не предполага разлика в позициите на членовете на делегацията.

Друго важно правило е да не се съгласявате веднага с предложената ви цена, дори и ако тя ви устройва. Направете пауза. Ако веднага дадете положителен отговор създавате впечатление, че партньорът ви е предложил много ниска цена и това може да го принуди да промени своята позиция: или ще се появят редица условия, които фактически да повишат цената, или подписването на договора може да бъде отлагано, а е възможно и да не бъде подписан. За да не се случи това – преговаряйте за цената. По същество или само проформа зависи от конкретния случай. Деловото общуване включва в себе си и способността да се правят компромиси. Основното правило на компромиса е: Преди да режете баницата, първо я увеличете! Колкото по широки са рамките на дискусията, толкова са по-големи са възможностите на страните безболезнено да компенсират отстъпките при решаването на основния проблем.

По време на преговори е допустимо да се използват само знаци, които са разбираеми за всички присъстващи. Неразбраните знаци могат да направят впечатление за "нечестна игра", затова трябва да се избягват.

Преговорите могат да се започнат с това, което ви обединява със събеседника. Например, времето (то е еднакво за всички) или с проява на внимание ("Как пътувахте?"). Останалите обстоятелства могат да ви разединят: политически събития и общи познати поради различното отношения към тях.

Членовете на делегациите не бива да напускат преговорите. Изключения могат да се правят само в случай, че е необходимо оказване на медицинска помощ. Ако излизат, за да получат допълнителна информация от своя екип, то това дава едностранно преимущество в преговорите, което не е етично. Ако се отлъчват поради служебни дела, то това е неуважение към партньорите, принизяване на тяхната значимост. Ако има нужда от информация може да се обяви почивка и тогава и двете страни могат да се възползват от това.

По време на преговорите ръцете на членовете на делегациите е необходимо да се намират върху масата. Известно е, че ръцете са източник на информация. Когато те са скрити, това подсъзнателно се възприема като напрегнато състояние на партньора. Спокойно лежащите на масата ръце означават спокойствие. Скръстените пръсти - защита, отбрана и т.н.

По време на преговори може да се пуши само при спазване на две условия: когато на масите има пепелници и е получено разрешение от присъстващите дами.

Записките в тефтери по време на беседа са станали традиция и ако не се прави това се възприема негативно. Затова е необходимо да се правят такива, поне за да не се обидят партньорите.

Препоръчително е да се избягва фамилиарност или фамилиарни и снизходителни жестове, от типа на потупване по рамото.

Ако след устна договореност е сключено и писмено съглашение, в което не са влезли моменти от устната договореност, то последните губят своята сила. Невключването в писменото съглашение на части от устните договорености никога не е случайно: "забравя се" това, което трябва да бъде забравено. Ако не ви устройва получения съкратен договор, не го подписвайте, а изпратете свой вариант. Или подпишете, но с приложен протокол за разногласията.

Устната договореност е равносилна на писмено съглашение само когато е сключена между първи лица (лидерите на преговарящите страни). За всички останали тя играе роля на протокол за намерения, тоест не е задължителна за изпълнение.

Следва продължение.

ПРИСЪЕДИНЕТЕ СЕ КЪМ БОЙНОТО БРАТСТВО!

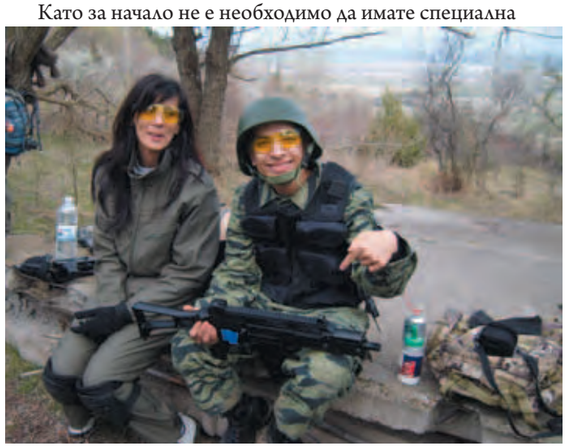
Да устоиш, да победиш, да докажеш своята сила и умения, да надделееш над противника или просто да оцелееш – към това хората се стремят от древни времена до днес. Спортът е жив пример за това – човек срещу човек, клуб срещу клуб, страна срещу страна, постижение след постижение. Спортът няма как да даде и стотна част от чувството, докато пълзите покрай поста на „противника", търсейки сигурно укритие, откъдето да атакувате.

Притеснението да не ви разкрият, желанието да стреляте първи и точно – ето тези чувства са неподправени. Толкова близо до реалността и в същото време си остава забавление и игра. Това е **Страйкбол или Airsoft** - командна «военна» тактическа игра, технология „откраднатa" от военните тренировъчни програми, създадена за максималното приближаване към реализма на бойните действия.

Каква е философията на страйкбола?

- Освобождаване на негативните емоции
- Премахване на агресията
- Изграждане на отборен дух и нагласа
- Толерантност към отбора, но и към противника
- ЧЕСТНОСТ, преди всичко!
- Спорт, екшън, адреналин, дисциплина, практически опит, комуникация с другите, взаимопомощ, благородство...
- И най-вече - ЗАБАВЛЕНИЕ

Като за начало не е необходимо да имате специална



подготовка или да притежавате специализирана екипировка. В играта могат да участват, както ветерани, така и абсолютни новобранци, които за пръв път са решили да опитат такова забавление. Ако не разполагате със собствена екипировка ще ви бъде дадена на място. Ако играта ви хареса и решите да участвате редовно можете да си закупите екипировка или да ползвате такава под наем. Последствията от това, че не сте играли до този момент могат да бъдат по честите ви „застрелвания", а може и да имате талант да оцелявате. Няма значение дали сте мъж или жена – забавлението е подходящо и за двата пола.

Подробности можете да откриете в кратък видео клип на адрес: **www.tv7.bg/news/69652.html**

Игрите варират от обикновени престрелки в оборудван полигон в гориста, полева местност или сгради, до



специално организирани и подготвени ролеви игри със сценарий. Как става това? Чрез добре режисиран сценарии, при който всеки да се почувства във „филма" и да преживее само неща, които са запазена марка за командосите и Холивуд! Ето един примерен сценарии, който се харесва много от участниците:

Задачата на групата е да освободи заловения от терористите лидер и да стигне до район, който се намира лагер на терористична група и да го унищожи. Тази задача е усложнена значително от липсата на достатъчно разузнавателни данни и от сложния за ориентиране терен.

Играчите разполагат с въоръжение и екипировка, но нямат достатъчно боеприпаси и средства за наблюдение. За щастие разполагат с достатъчно финансови средства, компас и карта, на която приблизително е отбелязано мястото, на което се намира пленен от терористите информатор! Той има важна информация и ако я ползват ще открият мястото, на което е скрита още информация, която значително ще улесни задачата им. За съжаление те ще имат възможност да му зададат само 5 въпроса. На 4 тях той ще отговори истина, а на един с лъжа!

Откривайки мястото на тайните ще трябва да следват инструкциите, написани на стената и да съберат пъзела, който ще ги отведе до следващата загадка!

По пътя за нея ще попаднат на възможност да купят три неща: Какви са те? Ще се разбере на място.

На следващото тайно място ги очаква нова изненада и ако не са успели да купят правилните неща ги чакат „страдания". Новите тайни ще им укажат правилния път за терористичната база, но за да разберат това ще трябва да открият тайник с важни предмети и нова информация!

И така нататък, докато не се стигне до най-важния проблем - как да победят лошите!

Забравих да кажа, че хората отговорни за ориентирането ще се изберат на произволен принцип и че през цялото време ще бъдете атакувани в произволен порядък от лошите. За щастие всеки елиминиран ще има възможността да се включи в боя пак! Само след 2 мин. (след намесата на медик).

И още... ако си откриете обяда ще ядете, ако ли пък не го откриете... само „Русенско варено"!

Успех!







Екип Профисек ЕООД

SWAT
(SPECIAL WEAPONS AND TACTICS)

Готови ли са специалните подразделения за високорискови операции, и да изпълняват функциите си по всяко време и на всяко място? Ако чакаме отговор на този въпрос тогава, когото от тази готовност ще зависят човешки животи т.е. в реална ситуация, е възможно да получим късен и то неприятен отговор. Естеството на дейността на специалните подразделения налага те да поддържат постоянно ниво на своята подготовка. Това ниво може да бъде проверено и контролирано от ръководителите на структурите, в които те са дислоцирани и става по няколко способа. Например чрез покриване на съответните нормативи или чрез изпити и тестове по специалността им. Най-добрата проверка и потвърждаване на високия професионализъм на тези хора, обаче става когото те се включат в директна надпревара, с подобни професионалисти и докажат пред всички, че с тях шега не бива!

В един прашен район на западните полупустинни райони на Америка, млади мъже с пистолети в тактически кобури на бедрата си и карабини в ръцете са готови да разберат кои от тях са най-добрите.

Това не е възстановка на прословутата престрелка в Додж сити през 1800 година! Това е американското национално SWAT състезание за 2010 г. организирано от Highlands Law Enforcement Training Center намиращ се близо до Литълтън, щата Колорадо! Това са мъже от всички краища на Съединените щати и от редица чужди държави. Те са там, за да тестват своите отбори, своята организация, оръжия и умения, физика и психическа устойчивост.

Създадено през 2007, само за няколко години неговите участници са вече над 30 тактически отбора. Целта е да сблъскат тактическите умения на участниците по време на изпълнение на дисциплини, аналогични с такива в реалния свят.

Общи елементи на всички дисциплини са екстремните физически натоварвания, преходи с оръжие и тактическа екипировка и всичко това комбинирано с предварително създадена тактическа обстановка и изпълнение на различни задачи.



В създаденото от Highlands Law Enforcement Training Center състезание са включени следните елементи:

1. Прочистване на сграда, с барикадирал се в нея въоръжен престъпник, откриване на ранен офицер и неговата евакуация до финалната линия.
2. Освобождаване на заложници в автобус. Упражнението започва с елиминиране на цел от снайперист и продължава с проникване и стрелба по мишени в автобуса и извеждане на заложниците;
3. Спасяване на ранен офицер. Отборът преодолява редица препятствия, стреля по различни мишени и накрая евакуира с носилка ранения офицер;
4. Стрелба с различни оръжия (пистолет, пушка, автомат) след прочистване и преодоляване на препятствия с противогаз;
5. Контра снайперска стрелба. Стрелба със снайперска пушка по различни цели, на различни разстояния, от различни позиции;
6. Стрелба с карабина и преодоляване на препятствия;
7. Стрелба с пистолет и противогаз при допълнителни физически натоварвания;
8. Интервенция с прикритието на тактически щит и стрелба с късоцевно оръжие.

Примерът на Highlands Law Enforcement Training Center е последван от редица организации в Съединените щати и през последните години се наблюдава изключително популяризиране на военните и полицейските приложни състезания.

Например:

1. South Eastern SWAT Association в Южна Каролина, организира SOUTHEASTERN SWAT COMPETION;
2. West Hartford Police Department организират Connecticut SWAT Challenge;
3. Harrisonburg Police Department от Пенсилвания имат SWAT Competition;
4. U.S. Shooting Academy организира U.S. National SWAT Championships.

Списъкът може да бъде продължен още поне с 10 – 15 организации, които организират подобни мероприятия за проверка на подготовката на полицейските структури и най-вече, за да се демонстрира пред широката общественост за какво се харчат парите на данъкоплатците. В България такава инициатива ще се проведе за първи път през есента на 2010 г. Фирма Профисек се е заела с амбициозната задача да организира и да срещне на огневата линия най-елитните полицейски и армейски групи, които имат подобни на американския SWAT задачи. Очаквайте на страниците на списанието актуални подробности за организацията, дисциплините и реда за провеждане на това събитие.





снимки: Department of Defense

Милен Иванов

ВТОРА НАГРАДА НЕ СЕ ПРИСЪЖДА

КАК ДА СЕ НАУЧИМ ДА СТРЕЛЯМЕ И ДА УЛУЧВАМЕ

Продължение от миналия брой

Както обещахме, в предишния брой на списание Professional, продължаваме статията за стрелба с огнестрелно оръжие.

Систематичността на тренировките в началния етап на обучението или, за да се поддържа вече достигнато ниво на подготовка трябва да има разумни граници. Напълно достатъчни са три тренировки седмично, с по 50-60 патрона. Всяка от тренировките трябва да включва няколко различни упражнения. В зависимост от поставените цели и постигнатите резултати обемът на тренировката може да се променя, но е по-полезно да се тренира три пъти в седмицата по 50 изстрела, отколкото един път в месеца по 1000 изстрела.

Най-добри резултати се постигат при работа с опитен треньор в стрелбище, а самостоятелното обучение дава, в най-добрия случай, възможност да се натренират само общи навици за работа с оръжието и стрелба. Всяко обучение се провежда постепенно, от простото към сложното. Задължително, като първи етап на обучението трябва да е общодостъпната методика за обучение на спортната стрелба. Преминаването към следващите етапи трябва да става само след като навиците и уменията за дадения етап са твърдо усвоени.

Добре е тренировките да се провеждат не в помещения (или поне не само в помещения), а на открито, защото такива условия за стрелба се срещат най-често в практиката. Това на свой ред усложнява процеса на обучение чрез влиянието и на външни фактори като вятър, различни условия на осветяване, непостоянна дистанция за стрелба, разлика във височината на стрелеца и целта, кръгов сектор за стрелба и т.н.

Стрелците обучавани в закрито стрелбище имат няколко много негативни особености на психо-физическата готовност за реални ситуации. Това произтича от изградения вече траен динамичен стереотип. При реална ситуация те допускат следните основни грешки:

1. Стрелбата с две ръце и липсата (или късите дистанции) на движение ги "заковава" на едно място и те не се движат, а се опитват чрез водене на огън да решат огневата задача;
2. Трайно усвоения навик да се стреля в строго определена директриса "натиска" раменете и им пречи да отворят сектора за обстрел. Такива стрелци не са свикнали да водят кръгово наблюдение и кръгово огнево покриване на целите;
3. Обучението с движение в стрелбищата води до изграждането на праволинейни навици за стрелба в движение. Там се отработват само упражнения напред и назад, и в най добрия случай крачка встрани и клек зад укритие. Липсва инстинктивна пространствена ориентация и чувство за "пласиране" и контрол на цевта с движение в необходимата посока.
4. Строгите мерки за безопасност в стрелбището (напълно необходими и задължителни) създават в стрелците много силен страх и респект към оръжието и посоката на стрелба. Това ги прави едновариантни при избор на тактически и огневи решения, в ситуации когато е важно да се порази целта на всяка цена. Например те не прибягват до използване на поразяващия ефект на рикошетите, до стрелба от различни нестандартни положения, над главите или между хората неучастващи в даденото въоръжено стълкновение. Наблюдава се и прекалена скованост и трудности в заучаването на определени похвати за стрелба.



5. При стрелба с големи денивелации (например при прочистване на стълбищни клетки) не могат успешно да се справят с различни по важност, височина и скорост цели.

Това са само няколко от проблемите, които възникват при еднотипно и традиционно обучение по стрелба в закрити стрелбища. В следващите статии ще се спрем по-подробно на този проблем.

Начини за стрелба с пистолет

Късоцевните оръжия (пистолет или револвер) са предназначени преди всичко за самозащита на техния притежател при мирни и бойни условия. За тези ситуации е характерно внезапното възникване на заплахата и необходимост от бърза реакции, която изисква мигновена оценка на ситуацията с едновременно отклоняване от линията на огън на противника, изваждане на оръжието, подготовката му за стрелба, прицелване и откриване на огън. Статични стойки при стрелба с пистолета в реална престрелка практически не се срещат, защото стрелбата се води на предлено къси дистанции 2-7 метра и приключва за секунди.

Процесът на стрелбата се състои от подготовка, прицелване и спускане. При обучението те се разглеждат отделно, но тези елементи са неразривно взаимосвързани. Когато стрелецът наработи усещане за оръжието, ги изпълнява автоматично, без да ги разделя. Тъй като за стрелба с пистолет остротата на зрението не играе толкова важна роля, като при стрелбата с пушка, зрителната памет и чувстването на оръжието, изработени при стрелба позволяват да се постигат значително по-добри резултати при стрелба с личния, пистолет, отколкото при стрелба с чуждо оръжие даже и от същия модел.

Подготовка

В началото ще разгледаме подготовката за бавна стрелба с една ръка, без ограничение във времето. Предполага се, че стрелецът държи пистолетът в дясната ръка. Най-важното при заемане на правилната стойка за стрелба – това е естествеността на положенията, минималното напрягане на мускулите, равновесието и устойчивостта на системата тяло-оръжие. Стрелецът застава с дясното рамо към целта, като раменатa са почти успоредни на директрисата. Краката са разтворени на широчината на раменете, пръстите на краката са завъртени лека навън, петите навътре. Тежестта на тялото е равномерно разпределена на двата крака. Гръбначния стълб е леко назад, за да се намали натоварването. Рамото на ръката с пистолета не бива да е прекалено повдигнато. Главата е завъртяна надясно по посока на целта. Тя трябва да се държи права без напрежение, без да се наклонява надясно или наляво, напред или назад. Ръката, която държи пистолета трябва да е напълно изпъната – като пред мишницата и мишницата трябва да са фиксирани без да са напрегнати. Допуска се леко свиване на ръката в лакътя, но тогава завъртането на тялото към целта трябва да е по-малко. Максимално отпусната лява ръка не трябва да пречи и може да е или свободно пусната надолу, поставена зад гърба, опряна на левия хълбок, сложена в джоба, сгъната в лакътя и притисната до гърдите (последното положение се използва най-често при стрелба от коляно).

Правилността на стойката се проверява по следния начин: заемете положението, насочете пистолета към мишената, затворете очи и отпуснете ръката с пистолета надолу. Без да отваряте очите, вдигнете ръката по посока на мишената и отворете очи. Ако пистолетът се е отклонил надясно или наляво от целта, тогава като преместите леко краката, променете малко ъгъла на завъртане на тялото по отношение на мишената и повторете проверката.

И накрая, за да продължите от тук нататък със стрелковите тренировки разберете кое е водещото ви око! За това, обаче, ще ви разкажем в следващия брой!

снимки: Department of Defense





Parabellum, по материали от Интернет

ПРОФЕСИЯ “СПЕЦНАЗ”

ВИНТОВКАТА ВСС “ВИНТОРЕЗ” – БЕЗМЪЛВНИЯТ ЛИКВИДАТОР

Винаги ми е правело впечатление, че S.W.A.T (Special Weapons and Tactics) частите на много страни всъщност не използват някакви особено специални оръжия, а просто “накичват” с различни аксесоари приетите на армейско въоръжение такива – тактическите ръкохватки, колиматорните и оптичните прицели, заглушителите, фенерите и т.н. придават техния страховит външен вид. На практика обаче повечето от използваното си е абсолютно стандартно армейско и полицейско въоръжение – и като конструкция, и като боеприпаси. Има обаче едно руско (всъщност съветско) оръжие, което напълно заслужено си е спечелило славата на оръжие за “спецназа”.



Разработена за нуждите на спец подразделенията в началото на осемдесетте години на миналия век под ръководството на конструктора Петър Сердюков, автоматичната винтовка ВСС (Винтовка Снайперская Специальная) “Винторез” си е спечелила славата на “снайперския автомат”. Чисто теоретично, това название звучи оксиморонно - концепциите “автомат” и “снайпер”са напълно различни една от друга, автоматът е за водене на бърз и плътен огън на относително къси разстояния, а снайперът е за прецизни изстрели на относително големи разстояния, като целта е всеки изстрел да бъде попадение. На практика обаче се е получило точно това – изключително ефективно на разстояния до 200 метра оръжие, способно да води точен, плътен и много смъртоносен огън.

От конструктивна гледна точка оръжието работи на принципа на газовата автоматика и е с ротационен затвор, имащ шест бойни упора. Цевната кутия е изработена от стомана чрез фрезоване с цел повишаване устойчивостта на конструкцията. Ръкохватката на затвора и лоста за промяна на вида на огън следват изцяло фейслифта на автомат “Калашников”. Ръкохватката на оръжието обаче е интегрирана в приклада както при снайперската винтовка “Драгунов”, като прикладът може да се снема от цевната кутия. В предната част на цевната кутия, след газовата камера, има няколко реда отвори, служещи за извеждане на част от барутните газове след изстрел, а останалата част служат за взеждане на затвора и презареждане. Най-интересната част от оръжието е заглушителят – той практически се явява и цев, с цел по лесно обслужване и компактност при пренасяне той може да се сваля, практически обаче няма смисъл да се стреля без него – защото оръжието практически няма цев. Освен това в самата концепция



на винтовката е заложено тя да бъде безшумна.

ВСС “Винторез”- устойство

Мерните прибори на оръжието са стандартни за руските оръжейни концепции – открити, като мушката е позиционирана в предната част на заглушителя – цев, а мерникът в предната част на цевната кутия, като е разграфен от “1” до “4” (за стрелба от 100 до 400 метра). Върху лявата страна на цевната кутия има планка за монтиране на оптически (или нощен) прицел - ПСО 1, с четирикратно увеличение, като мерната скàла е премаркирана за патрона на оръжието – 9х39 СП-5, СП- 6.

И като споменахме патрона, смятам, че си заслужава да му обърнем специално внимание. Създаден на базата на съветския 7.62х39, този боеприпас има 9-милиметров куршум - 9х39 и две разновидности - СП-5 (с обикновен куршум) и СП- 6 (с бронебоен куршум). Куршумите и на двата боеприпаса са



дозвукови още при излитането си от цевта на оръжието – началната скорост е около 280 м/с, но поради големия си обем и маса (около 16 грама) предизвикват изключително тежки наранявания.

Пълнителите на оръжието са два вида: с вместимост 10 и 20 патрона, като интересно е, че пълнителят влиза дълбоко в цевната кутия на оръжието, като целта е да се намали височината му с поставен пълнител и да се постигнат по-добри възможности за стрелба от легнало положение.

ТТ ДАННИ НА ОРЪЖИЕТО:

Калибър: 9х39 мм
Дължина: 894 мм
Височина: 160 мм
Ширина: 40 мм
Маса без патрони и оптически прицел: 2,6 кг
Маса с патрони и монтиран прицел ПСО-1: 3,41 кг
Маса с патрони и прицел НСПУ-3 (нощен прицел): 5,93 кг
Темп на стрелба: 600 изстрела в минута
Скорострелност: 40-100 изстрела в минута
Начална скорост на куршума: ~ 290 м/сек
Прицелна далекобойност с оптически прицел: 400 метра
Прицелна далекобойност с нощен прицел: 300 метра
Вместимост на пълнителя: 10, 20 патрона

В заключение - сигурно вече си задавате въпроса: “Добре, какво всъщност му е “специалното” на това оръжие”? Ами специалното е, че с него се действа в изключително екстремални условия – когато бързо и тихо трябва да се ликвидират един или повече обекти, представляващи непосредствена заплаха. Например: снайперска двойка се придвижва за заемане на позиция – снайперистът със СВД, спотърът (както е модерно да се казва днес) с “Винторез”. При изненадваща поява на един или повече неприятели спотърът може да ги елиминира бързо и тихо – оръжието води напълно автоматичен огън. Неприятел стои на КПП и пречи на преминаването на диверсионна група – трябва тихо да се елиминира. Обект се охранява с кучета... И така-нататък...

С тези задачи “Винторез” се справя прекрасно, което без съмнение го прави един истински “спецназ” във въоръжението...

ЛОВНИ КАРАБИНИ „ТОМПСЪН ЦЕНТЪР”

Оръжейната фирма „Томпсън Център” е създадена през 1965 г., когато Томпсън Тул търси ново оръжие, което да започне да произвежда. В същото време оръжейният конструктор Уорън Център търси производител на своя пистолет „Кънтендър” (Contender). Така на бял свят се появява новата фирма, носеща имената на създателите си – Thomspon/Center.

В момента фирмата предлага най-различни модели ловни карабини, включително и такива с предно пълнене. Въпреки че „Томпсън/Център” е сравнително нова компания, само за 40 години нейните продукти допринасят значително за развитието на спортната стрелба в САЩ, а ловът с еднозарядни пистолети и карабини с предно пълнене е възроден отново. И днес фирмата запазва водещата си роля в тази област благодарение на стремежа си към създаването на иновативни и качествени продукти за любителите на лова. От 2007 г. насам „Томпсън/Център” става част от „Смит и Уесън Холдинг Корпорейшън” и е в основата на успеха на новите ловни пушки с марката „Смит и Уесън”. Фирмата е специализирана и в производството на висококачествени цеви за различни видове ловни пушки и карабини, които са признати за едни от най-добрите в Щатите.



Ще започнем представянето им с полуавтоматичната ловна карабина R55 „Бенчмарк” (Bencmark), която е предназначена за лов на дребен и среден дивеч, както и за развлекателна стрелба по мишени. Автоматиката и се основава на принципа на отката при неподвижна цев, като ръкохватката за зареждане е от дясната страна на цевната кутия. Характерното за нея е липсата на мерни прибори, като се използва само с оптика, която се монтира върху интегрираните в задния край на цевта две малки шини тип „Уийвър”. Прикладът е ергономичен, с добре очертана полу-пистолетна ръкохватка, гумен задтилък и се изработва от ламинирана дървесина в едно цяло с ложата. Цевта е от оръжейна стомана, спортен тип, изключително прецизно изработена и с висока точност. Тя и останалите метални части са с тъмносиньо антикорозионно покритие с изключително високи качества, което позволява използването на оръжието при всякакви климатични условия. Карабината е с механичен предпазител, намиращ се в задната част на спусковата скоба, както има и антабки за поставяне на ремък. Използва метален пълнител, който стандартно е за 10 патрона, но могат да се поръчат и 5-зарядни.

„Бенчмарк” е предназначена за популярните в цял свят малокалибрени ловни патрони .22 LR (Лонг Райфъл) с периферно възпламеняване. Цевта е дълга 457 mm, като общата дължина на оръжието е 762 mm, а теглото 3 kg. Вече може да се намери и у нас на цена около 1300 лева. Следващите няколко ловни карабини са модели от серията „Енкор”, предназначени за лов на дребен, среден и едър дивеч, което зависи от подбрания калибър. Те се характеризират с това, че са еднозарядни, със задно пълнене и се зареждат, като се издърпа надолу спусковата скоба и се пречупи цевта. Ударно-спусковият механизъм е конструиран така, че цевите могат да се сменят, като по този начин една основа може да използва различни по калибър цеви, което позволява да се ловува на различен дивеч. Това става, като се избие щифта, закрепващ цевта към цевната кутия. Спусъкът е класически и регулируем по разстояние. Чукчето на ударника е открито и с назъбена горна повърхност, за да може да се взвежда по-лесно при лошо време или когато се използват ръкавици.

Снабдени са с регулируеми механични мерни прибори, но има и без такива, като се използват само с оптика. Естествено предвидена е възможност за поставяне на оптика и на оръжията със стандартни прибори. Прикладът и ложата на част от моделите се изработват от американски орех отделно, като прикладът е ергономичен, тип „Монте Карло” с удебелен гумен задтилък и ярко изразена полупистолетна ръкохватка. Повечето модели обаче са с ложа и приклад от синтетика в различни камуфлирани разцветки или в черно. Карабините са снабдени и с антабки за поставяне на ремък. Предлагат се в около 95 варианта в зависимост от калибъра, като се започне от малокалибрените .17 Хорнеди Магнум Римфайър (.17 HMR), премине се през няколко средни калибъра като .308 Уинчестър (.308 Win.) и се стигне до мощните .375 Холанд&Холанд (.375 H&H). Разлика има и в дължината на цевите и покритието им – сребристо и тъмно синьо, което от своя страна влияе върху общата дължина на оръжията и теглото. В таблицата са дадени двата основни варианта на карабината, а на снимковия материал са показани основните модели в зависимост от приклада, цвета, разцветките и мерните прибори.

Калибър	.17 HMR	.204 Ругер
Дължина на цевта, mm	610	660
Обща дължина, mm	978	1029
Тегло, kg	2,77	3
Вместимост, бр.	1	1











гр.София, р-н Триадица, м."Жил. група Южен парк", бл. 28,
evronorm_bg@abv.bg, тел./факс: 963 00 65

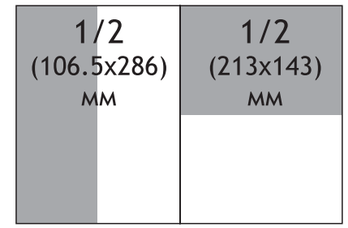
РЕКЛАМНА ТАРИФА PROFESSIONAL

Реклама- корица
2-ра и 3-та - 900 лв.
4-та - 700 лв

Реклама - тяло
1 страница - 600 лв.
1/2 страница - 300 лв

Рекламна страница с PR материал
1 рекламна стр. + 3 текстови - 900 лв.
1 рекламна стр. + 5 текстови - 1 200 лв.

Отстъпки за участие в издание
2 бр.-15%
3 бр.-20%
4 бр.-30%



Формат	210/280 мм обрязан
Тираж	3000 бр.
Хартия тяло	80 г/м^2 LWC
Корица	170 г/м^2 хром/мат с UV лак
Печат	4+4

Формат на изображенията: PDF, EPS, TIF 300 dpi. Текстовете да са обърнати в криви.
Размер на 1 страница: обрязан формат 210x280 мм, необрязан формат 213x286 мм

Запазени знаци, лога, марки - векторизирани във формати, *.eps, *.ai, *.cdr.
Излиза между 1-о и 5-о число на месеца. Заявки за реклама се приемат до 1-во число на предходния месец.

Цените са без ДДС. Авансово заплащане 50%.

Екип Профисек ЕООД

РИСКОВЕ И ОПАСНОСТИ ПРИ ЕКСТРЕМНИТЕ СПОРТОВЕ

Историята на екстремните спортове започва през 80-те години на миналия век, когато от различни краища на света младите хора започват да практикуват и да измислят нови и по-различни начини да се забавляват сред природата. И ако в началото шокират обществото или ентусиастите попадат зад решетките, то за няколко години успяват да се наложат и да привлекат милиони последователи.

С годините видовете екстремни спортове стават все по-многобройни и различните дисциплини се борят за популярност и оригиналност, а техните последователи непрекъснато нарастват.

Ето и някой от най-популярните: кънки пързаляне, сноуборд, скално катерене, планинско колоездене, бънджи скокове, парапланеризъм, парашутизъм, различни видове летене с леки и свръх леки летателни апарати (снабдени или не с двигател), рафтинг, гмуркане, сърф, сноуборд, кайтборд, скейтборд, пейнтбол, еърсофт, офроуд и т.н.

Естествено това е много малка част от видовете екстремни спортове и всеки един от тях притежава и завладява с индивидуалност и предизвикателност.

Тук трябва да отбележим и не бива да се забравя, че тези спортове макар и пълни с приключения, са опасни за живота и здравето на практикуващите ги, ако те не спазват строго правилата за тяхното практикуване. И макар да се спазват правилата на играта, статистиката показва, че рискът и травматизмът при тях е по-висок, отколкото при обичайните видове спортни забавления!

Вредата от заседналия начин на живот е очевидна. А какви са рисковете от неразумното практикуване на различните екстремни спортове? Тези модерни забавления са по-рискови, по-адреналинови и опасни. Маутънбайкърите, карат велосипеди по много стръмни наклони, фриирайдърите са скиори, които се спускат по особени трасета, почитатели на бънджи скокове и др. Всички тези дейности се случват винаги далеч от компетентна медицинска помощ и понякога единствената надежда при пострадали е те да се открият и транспортират навреме до подходящо болнично заведение, и то след като им е оказана навременна и компетентна първа помощ.

Всеки спорт е хубав, когато е аматьорски и се практикува за удоволствие. Вредно е когато се прекали с неблагоразумието и натоварванията, когато не се вземат предварително всички предохранителни мерки.

Хората, които практикуват екстремни спортове, трябва да са наясно, че опорно-двигателният апарат на човека е структура, която не е предвидена за екстремни натоварвания, които са извън нормалните възможности. В противен случай може да се стигне до травматизъм, който да се отрази доста пагубно след определен период години. С течение на годините рисковете от травми нарастват.

Според статистиката на планинската спасителна служба към БЧК за през 2006 г. е оказана помощ на 1069 души, от които 703 са откарани в болница с тежки увреждания. Разпределението по видове дейности в планините, при които е получена травмата, е следното: ски-спорт – 991 случая, сноуборд - 125 случая, туризъм, алпинизъм, парапланеризъм и планински велосипеди - общо 54 случая. Най-силно засегнати от планинския травматизъм са младите хора на възраст от 21 до 30 години с 267 случая. През едногодишния период, извън редовните дежурства, в ПСС са проведени 53 спасителни акции, с участието на 429 планински спасители. Оказана е помощ на 41 пострадали, 12 са намерени здрави и са изведени от критична ситуация. Седем туристи са намерени мъртви, като телата им са транспортирани от планините до медицинско заведение при сложни теренни и метеорологични условия.

Според една статистика на Американската Асоциация по делта и парапланеризъм, смъртните случаи при екстремните спортове са много редки, особено в сравнение с някои добре познати професии. Ето извадка от нея:

1. Пожарникар - 49 на 100 000
2. Доброволец от Корпуса на мира - 43 на 100 000
3. Шофьор на камион - 40 на 100 000
4. Височинен работник - 32 на 100 000
5. Делтапланерист - 22 на 100 000
6. Шофьор на лека кола в САЩ - 20 на 100 000
7. Парашутист - 2 на 100 000

Според класацията на сп. "Форбс" в световен мащаб класацията е такава:.

1. Бейсджъмпинг; 2. Хелискийнг; 3. Дайвинг; 4. Кейв-дайвинг; 5. Булрайдинг; 6. Сърфинг; 7. Стрийтлагинг; 8. Алпинизъм; 9. Екстремен велокрос; 10. Рафтинг

Може би изводът е, че ако си падате по някой от тези великолепни спортове, най-добре е да опитате. Просто преди това се запознайте с потенциалните рискове и спазвайте мерките за безопасност. Задавайте много и смислени въпроси на своя инструктор преди, след и по време на занятията, обучавайте се при квалифициран и надежден инструктор, и помислете за добра застраховка!

RENT AND SALE - 02 / 480 40 00, 0888 955 544



PROJECT:

AMFION LTD.
BUILDING WORKSHOP

02/964 12 80
0886 885 788
FAX: 02/963 35 57
WWW.AMFION-BG.COM

OFFICES

SHOPPING AREAS

PARKING PLACES



ПРОФИСЕК

ПРОФЕСИОНАЛНА СИГУРНОСТ

РИСК МЕНИДЖМЪНТ

ФИРМЕНА СИГУРНОСТ

ЗАЩИТА НА ИНФОРМАЦИЯТА

СИСТЕМИ ЗА СИГУРНОСТ

website: www.profisecbg.com
адрес: гр. София, ул. Бигла 16А, вх. Б
тел./факс: 02/962 05 23