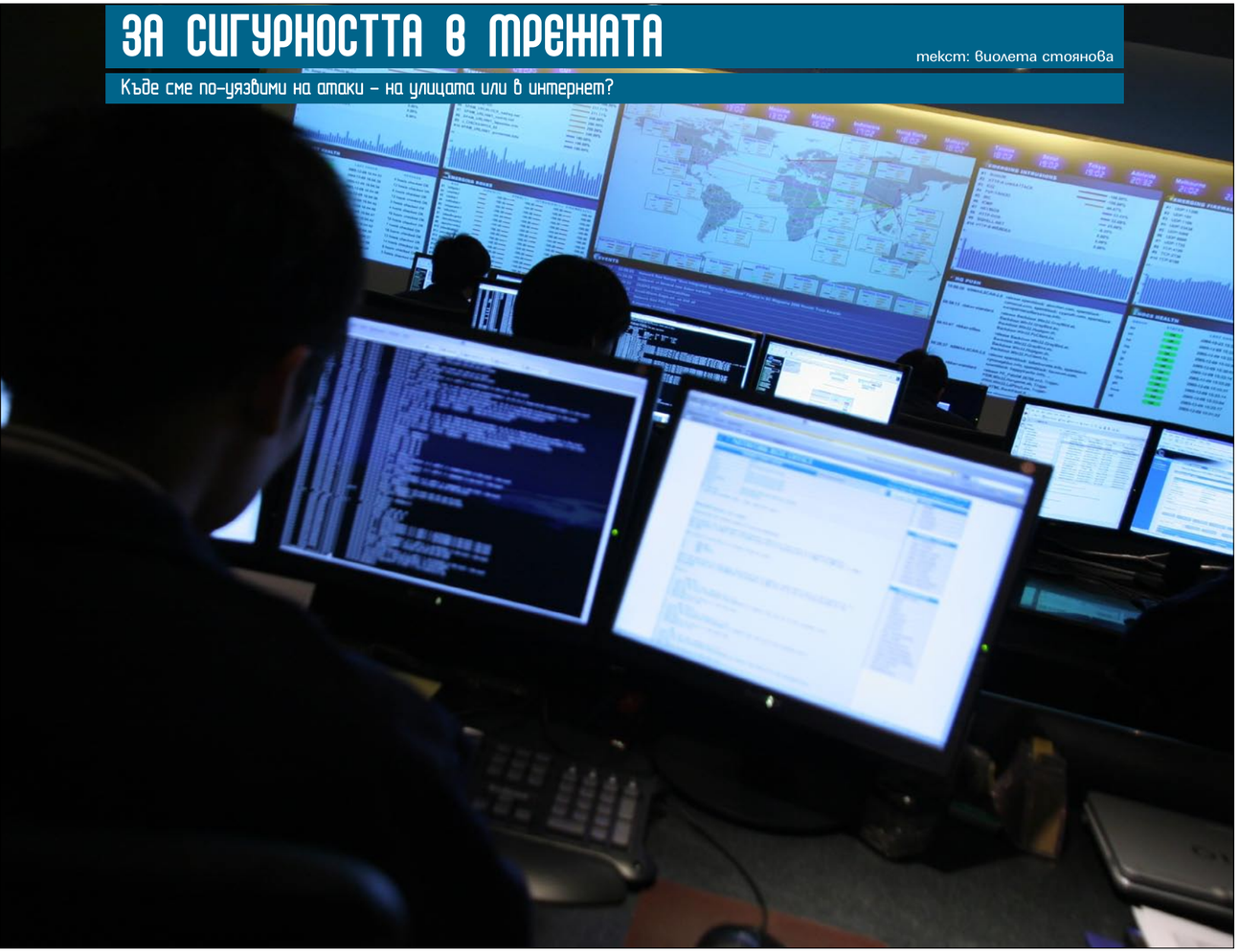
ЗА СИГУРНОСТТА В МРЕЖАТА

текст: виолета стоянова

Къде сме по-уязвими на атаки – на улицата или в интернет?



Безсмислено е да обяснявам какво означава да си част от Глобалната мрежа. Не защото няма какво да кажа, а защото има риск да отегча мнозина от вас. Сигурна съм, че точно вие, които четете списание HiComm, много добре осъзнавате зависимостта на съвременното общество от интернет свързаност, мрежи и т. н. Само се замислете каква част от ежедневието ви преминава във виртуалното пространство, седейки пред монитора? Отговорът всъщност няма значение – за някои може да е плашещ, за други – повод за гордост. Всъщност, макар и да звучи малко налудничаво, съвременното общество живее във виртуалното пространство – там то се забавлява, общува, създава нови приятелства, играе на игри, намира различна информация, чете книги, поръчва си храна, купува дрехи, работи... Ненапразно за "Личност на година за 2006" списание Time посочи не Бил Гейтс, не Джордж Буш или който и да било герой на нашето време, а You. Ти, който си отсреща. Ти, който си част от обществото, съставящо съдържанието в интернет. Или най-вече ти, който сам избираш какво да четеш, как да се забавляваш и изобщо как да осмислиш присъствието си в Глобалната мрежа. Битуването ни във виртуалното пространство има много аспекти, но като че ли най-малко засегнат остава въпросът за сигурността ни в него.

risk N1

Малко са хората, които си дават реална сметка какви са рисковете и опасностите във виртуалното пространство. Обикновените потребители, т. нар. "юзъри", не се интересуват от това, как функционира дадена технология, какви са нейните предимства и съответно пропуски. Важното за тях е тя да работи и чрез нея те да вършат своята работа. Точно тук идва основният пропуск в системата. Неслучайно най-известният хакер в света Кевин Митник определи **човека като най-слабото звено в компютърната система.** И ако се заинтересувате, сигурна съм, че ще откриете не един или два случая на катастрофи, аварии, компютърни сривове, източване на информация и др., основна причина за които е факторът, наречен "човешка грешка". 80 на сто от всички инциденти по море също се дължат на човешка грешка, както и спирането на атомен реактор в Япония. Дори фаталната катастрофа в атомната централа в Чернобил вероятно е плод на човешка грешка.

В компютърен аспект човекът е не по-малко уязвим от рискови ситуации. В повечето случаи той трудно може да се предпази по-

ради неспособността си да оцени правилно степента на риск. Или с други думи казано, трудно преценява коя информация е конфиденциална и коя може да споделя в интернет, кои интернет страници генерират спам, предават и заразяват компютърните системи с вируси, къде се дават личните данни, както и с какви средства и механизми могат да се предпазят от евентуални атаки. Именно подобни слабости създават благоприятно поле на действие на немалко хакери, кракери и т. н.

Основната предпоставка за атаки е незнанието. **Защото, когато не знаеш за дадено нещо, не означава, че то не съществува.** Последствията от това незнание могат да се окажат фатални не само за обикновения потребител, но и за водещи фирми и компании. В някои случаи е достатъчно един служител да издаде конфиденциална информация и системата е почти разбита. Дори понякога за целта не е необходимо използването на компютърни трикове. Една от атаките, която не е свързана с техниката, Митник нарича **"социално проучване"**. Тя се състои в убеждаването на някой по телефона или чрез e-mail-а да ти даде нужната информация, например номера на кредитната ти карта. Много по-лесно е да получиш информацията, от която се нуждаеш от даден компютър, като просто заблудиш човека, който го използва. Разбира се, начините за проникване в системата са много и за да се предпази от тях, човек трябва да е наясно с тяхното съществуване. Защото независимо с колко дебели стени и системи за сигурност е обграден един бизнес, много по-лесно той може да бъде разбит отвътре – от фактора, който не се вижда и за чието съществуване не се знае. Затова практиката днес налага едно много разумно решение – наемането на консултантски фирми, осигуряващи защита и сигурност на бизнеса – от средствата за физическа охрана до ИТ експерти по сигурност.

експертно мнение

По въпросите за ИТ сигурността потърсих коментара на Йовко Ламбрев – личност, която се спряга в редица области от фотографията, изкуството, идеята за отворен код, блог пространството и не на последно място в сферата на ИТ сигурността.

Каква е позицията на бизнеса спрямо ИТ технологиите за сигурност?

Ако допреди 5–10 години информационните технологии стояха поскоро встрани от основния, т. нар. соге бизнес, то сега те са част от него. Затова става все по-критично съвременните системи да работят добре. На практика това е жизнено необходимо. Ако те спрат, означава загуба на пари, време и нерви. Другият аспект е, че ставайки част от самия бизнес, внедряването на съвременни технологии вече не е лукс, а инвестиция. Доколко голяма ще е тя, зависи от нуждите на самата фирма.

Коя е най-голямата заплаха за бизнеса?

Това са хората, които взимат решенията, или т. нар. decision makers, и по-точно тези, които не осъзнават необходимостта от инвестиране в сигурността на бизнеса си. Всъщност това е един вид форма на застраховане, но в повечето случаи се възприема като форма на рекет. Обикновено на тези хора им е трудно да осъзнаят проблема и да си отговорят на въпроса, защо трябва да инвестират в нещо, което не е осезаемо. За тях буквално нищо няма да се промени след тази инвестиция, но истината е, че има промяна, дори тя да не се вижда. Може би българският бизнесмен не се страхува достатъчно, но проблемът е, че когато такова нещо се случи, вече е късно. Определено никоя българска банка няма да е щастлива, когато се случи първият сериозен банков обир. По отношение на сигурността това е проблем, който силно касае нашите географски ширини и е силно подценен.

Какви са предизвикателствата, които стоят пред фирмите?

Отговорът е комплексен. Фирмите са изключително уязвими в интернет. През мрежата е най-лесно да се достигне до корпоративната информация, особено когато никой не забелязва, че операционната система е оставена 3 години на произвола на съдбата. Все някой трябва да се грижи за нея, да я наблюдава, тъдейтва или замяна с нова версия. Същевременно трябва да се прецени достъпът до корпоративната информация – на кои хора какъв достъп им е необходим. Основен проблем в повечето фирми е, че никой не следи движението на хората във фирмата. В момента за целта все повече назрява идеята за налагане на т. нар. identity management като част от системата за сигурност. Служителят, постъпвайки на работа, получава виртуално ID под формата на виртуална лична карта и към нея съответно да се добавят или отнемат определени нива на достъп в системата в зависимост от текущата му позиция.

Къде са слабите места за проникване?

Голям процент от хората, общуващи по интернет, се доверяват на имейла си априори. А това е изключително елементарно за атака – почти всеки току-що проходил кракер може да подмени подателя на едно писмо и да изпрати съобщение, което да заобиколи защитите. Не са малко случаите на т. нар. фишинг измами – кражба на финансова и конфиденциална информация през интернет. Получавайки фалшиво писмо от неговата банка или компанията, в която работи, потребителят лесно се подлъгва, предоставя личните си данни и се оплита в мрежата. Разбира се, има много начини да се открие номерът на кредитната карта. Мой колега например си откри копие на фактура в интернет, на която присъства номерът на кредитната му карта, което е недопустимо.

Как да се предпазим от подобни атаки?

От една страна, човешката природа е доста доверчива. Съответно за хората, които се появяват в интернет, мрежата е нещо изключително интересно. Място, в което те ще намерят само хубави неща. И това е нормално. Човек, като се разхожда из улиците, не очаква задължително да бъде нападнат, обран или пребит. Обаче се случва. По същия начин подобни неща се случват и в Интернет. Хората, които се разхождат по улиците, присъстват и в Интернет, **т. е. виртуалният и реалният свят вече не са нещо различно.** В никакъв случай не искам да кажа, че трябва постоянно да дебнем за атаки, но е хубаво да сме внимателни, да преценяваме къде наистина се изисква да дадем личните си данни и къде не. Същевременно можем да се застраховаме с немалко технически средства. Например много е полезно използването на електронен подпис при изпращането на оферти, документи и др. Друг вариант е т. нар. система за публично-частните ключове PGP, която генерира двойка ключове с помощта на програмата, която използва. Частния ключ човек винаги пази някъде при себе си, а публичният се изпраща на т. нар. "Key" сървъри ключове в интернет. Начините са много, важното е да се изгради култура на ИТ сигурност.