Кибер сигурността през очите на обикновения потребител. Добри практики.

Всеки иска организацията му да бъде ефективна и защитена. Повечето експерти по киберсигурност в света се съгласяват, че независимо от защитите и нивото на контрол е просто въпрос не на мерки за сигурност, а на време - кога ще бъде осъществен пробив. И така докато експертните екипи по киберсигурност се борят всекидневно с непрекъснато развиващите се външни атаки, сега те също са отговорни за справяне и с риска от вътрешни нарушения (пробиви). Истината е, че по-голямата част от организациите ще се сблъскат с някакво нарушение (пробив), независимо дали става въпрос от външни актьори или от вътрешни заплахи.

За да сте сигурни, че сте подготвени е изключително важно да направите плавен подход към сигурността на организацията си. Има добри практики в сферата на киберсигурността, които може да не сте обмисляли до сега, но определено трябва да ги зачитате.

1. **Прилагане на формален подход за управление на информационните системи.** На първо място е добре да се стартира със създаването и поддържането на **рамка за информационната сигурност**, която да е в съответствие с вашата стратегия за развитие. Трябва да сте уверени, че програмата ви дава възможност да използвате подход, базиран на риска и да даде възможност на вашите екипи да откриват инциденти, да разследват ефективно и да реагират бързо.
2. **Спиране на загубата на данни.** Повечето предприятия разчитат на доверието на служителите си, но това няма да ги спре да напускат компанията. Истината е, че потребителите крадат данни. Неотдавнашно проучване на повече от 1500 специалисти по сигурността установи, че извличането на данни от дадена крайна точка е най-важната загриженост за сигурността на 43% от тях. Сега повече от всякога е изключително важно да контролирате достъпа, да наблюдавате доставчиците и изпълнителите, както и служителите и да знаете какво правят потребителите с фирмените данни, за да намалите тяхното изтичане.
3. **Разпознаване на вътрешни заплахи.** Служителите са най-големия актив в предприятието, но също така могат да бъдат и вашия най-голям риск. Дори след проведено добро обучение на потребителите, за да бъдат вашата линия на сигурност и защита, все още се нуждаете от технология като последна линия на защита. Наблюдението на активността на потребителите ви позволява да откривате неразрешено поведение и да проверявате дали действията на потребителите не нарушават правилата за сигурност. Вътрешните заплахи могат да останат незабелязани, но фактът, че става дума за нарушения (пробиви) могат да струват изключително скъпо.
4. **Редовно архивирайте вашите данни.** Тази практика често е пренебрегвана както от потребителите, така и от много компании, които смятат архивирането на файловете за безсмислено. Но всяка организация ударена с **ransomware** (***ransomware** - вид злонамерен софтуер от типа на крипто вирусите, които имат за цел да публикуват данните на компанията/потребителя или да ограничат достъпа до тях чрез заключване в случай, че не е платена определена сума.) от сорта на “Wannacry” или “Petya”, може да ви каже колко е

важно да гарантирате изпълнението на тази най-добра практика. От съществено значение е организацията да има пълно архивно копие на цялата работна информация, не само от гледна точка на добрата хигиена на сигурността, но и за справяне с възникващи атаки.

5. **Пазете се от Социално инженерство.** Технологиите и политиките за информационна сигурност, които се въвеждат не заменят нуждата от разума и не премахват човешката грешка. Тактиките за социално инженерство се използват успешно от десетилетия, за да получат информация за вход и достъп до криптирани файлове. Опитите могат да идват както от телефон, така и по мейл или друг вид комуникация с вашите потребители. Най-добрата защита е да образовате и обучите своите потребители.
6. **Обучение и образоване на потребителите.** Независимо колко са талантливи и можещи вашите потребители, те винаги ще бъдат най-уязвимото и слабо звено, когато опре до информационна сигурност. Това не значи, че не можете да снижите риска с редовни обучителни и образователни курсове по кибер защита и добри практики в тази област. Обученията трябва да са в направление от сорта на как да се разпознава **phishing*** (**phishing** - злонамерен опит за придобиване на чувствителна информация, като потребителски профили и пароли и др., с цел злонамерени действия); как да се правят силни пароли; как да се избягват опасни приложения; как да се подсигури и да се гарантира, че ценната информация не се изважда извън компанията в допълнение към други важни рискове за сигурността на потребителите. В подобни обучителни сесии може да се почувствате така, сякаш поставяте хората си в неудобно положение, но обучението ще доведе до правилна хигиена на киберсигурността, която е от критично значение. Намирането на правилна и креативна техника/методология за обучение също е полезна в тренировъчния процес.
7. **Оформете добра и ясна политика за нови служители и 3-ти лица.** Компанията трябва ясно да обособи практиката в областта на информационната сигурност, както и изискванията и очакванията към потребителите, когато се назначават. Това обикновено се залага в договора при назначаване.
8. **Обновявайте софтуера и системите.** Кибер престъпниците изобретяват нови техники и зловредни приложения ежедневно, като търсят уязвимост навсякъде по системите и софтуера. През 2014г. имаше много шум около така наречения **Heartbleed BUG -** мрежови бъг, с който се извършиха огромни пробиви в множество системи на десетки организации сред които Amazon, GitHub, Pinterest, цялата Wikipedia, Origin, Sony Online Entertainment, Steam, Android 4.1.1, Mozilla Firefox и много други.
9. **Изгответе списък/лист със случилите се инциденти и справянето с тях.** Колкото и добре да прилагате добри практики в киберсигурността винаги има шанс да ви пробият отново. Между другото ако разполагате с вече добре изграден план за справянето с пробивите на база списъка със случилите се инциденти, ще можете на практика да се защитите от всички опити за пробив с подобни злонамерени софтуери, с които вече имате опит. По този начин ще ограничите последиците от евентуален пробив (или ще го елиминирате) и ще ви позволи да се възстановите ефективно.

10. **Поддържане на сертификати/стандарти за сигурност.** Сертификацията също е важен процес да пазите конфиденциалните си данни. По един или друг начин това е още една степен на защита обвързана с ежегодни проверки на потребителите, изгражда се система на работа, правила и поведение по определен стандарт, който дава допълнителна гаранция в комбинация с гореизброените точки, че ще се постигне висока степен на умения по киберсигурност на ниво потребител. Освен това одитирането, пазенето на log файлове с потребителски коментари във връзка със съмнения за пробив или изтичане на информация също е от важно значение.

Има и съществуват безброй добри практики в областта на киберсигурността и това са само някои от тях, които се смятат за едни от най-важните.

Пример от практиката за USB DROP

Това може би е един от най-разпространения пример за потребителска небрежност и дори до някъде некомпетентност породена от ниската степен на образованост и липсата на добро вътрешно обучение по кибер защита. Социалния експеримент е проведен от американска компания за 3 месеца. Приложението на експертимента включвало изпускане на 200 броя USB флаш памет на обществени места с висока посещаемост като заведения за бързо хранене, кафенета, ресторанти, паркове и градини, публични площади и др. Всяко USB е било в различен цвят, без надписи по него, но с предварително подготвен текстови файл в него, с проследяващ линк и контакти с “притежателя”- мейл и телефон, както и софтуер, който показва, че флашката е пусната в компютър. Резултата от експеримента е много потресаващ. Всички флашки без изключение са включени в компютър както на работното място така и в дома, като дори някои от хората намерили флашките потърсили контактс с “изгубилия” флаш паметта и дори попитали дали има вирус във преносимата памет. Още по-покъртително е, че 34 броя от флашките са пуснати от специалисти работещи на летището в Сан Франциско, както и няколко охранителни служители в сградата на Гугъл.
По подоен начин, чрез вируса **“Stuxnet”**, от типа на червеите, който САЩ и Израел използваха да инфилтрират Иранската ядрена програма през 2010г.

Атанас Радев
ЦИНСО-БАН