РАБОТАТА ОТ РАЗСТОЯНИЕ – ВЪЗМОЖНОСТИ И ПРЕДИМСТВА, ЗАПЛАХИ И РИСКОВЕ ЗА ИНФОРМАЦИОННАТА СИГУРНОСТ

Въведение

Епидемията от вируса COVID 19 и свързаните с нея ограничения на социалните контакти промениха бързо и силно социалната и икономическата среда,, което принуди организациите да приложат нови методи за осъществяване на своята дейност.

Един от тези методи е **работата от разстояние** чрез използване от служителите на различни **преносими собствени и служебни ИТ устройства** за изпълнение на своите задължения.

Това позволи на много от организациите да запазят работоспособността си и да продължат да функционират, но **силно повиши рисковете за кибер сигурността.**

Използване на свои собствени устройства
(Bring Your Own Device – BYOD)

Освен за лични нужди, при изпълнение на служебните си задължения, служителите използват собствени преносими устройства като смартфони, таблети, лаптопи за достъп до мрежите и информация на организациите.

Прилагането на модела BYOD носи удобства и води до повишаване на ефективността на работата на организациите, но увеличава значително рисковете за кибер сигурността.

Защо моделът BYOD представлява проблем за сигурността

Преносимите устройства се превръщат в проблем за сигурността по много начини, някои от които са:

- кражба или загубване на устройства;
- устройства, съдържащи чувствителна информация, са продадени или рециклирани;
- използване временно или инцидентно на устройствата от неоторизирани лица;
- устройството е компрометирано при инсталиране на приложение, заразено с малуер;
- устройствата нямат адекватни системи за сигурност;
- "човек по средата" - когато трета страна следи трафика или подслушва комуникациите,
- и др., като например:

Използване на предпочитан софтуер

Служители имат на своите устройства предпочитан софтуер, който използват за изпълнение на дадени служебни задачи.

Този модел на употреба на софтуерни продукти (операционни системи и приложения), често наричан „Bring Your Own Application – BYOA“, е резултат на факта, че навиците и предпочитанията на потребителите се променят трудно.

Това е съществен проблем по отношение на сигурността на преносимите устройства, с който се сблъскват организациите, най-малко поради следните причини:

- предпочитаните приложения може да не са най-ефективните за изпълнението на дадена работа;
- продуктите, получени с нестандартните приложения, може да са трудни за разчитане или използване от останалите колеги на служителя;
- предпочитаните приложения може да са по-несигурни, отколкото стандартните приложения, използвани в организацията;
- предпочитаните приложения може да са незаконни, което може да подложи организацията на риск от нарушаване на законите за авторски права.

Управление на сигурността при BYOD

Съществуват няколко различни стратегии за сигурност за BYOD, които могат да бъдат приложени от организацията:

- да не се прави нищо: свободен режим за използване на мобилни устройства, които стават все по-мощни, но и носещи повече опасности;
- изцяло се забранява се достъпа до корпоративната мрежа чрез мобилни устройства; подход, носещ най-голяма сигурност, но водещ до намаляване на ползите за организацията и до раздразнение за служителите;
- лимитиране на използването на мобилни устройства до някои дейности, например достъп до електронната поща и до календарите;

- лимитиране на броя на хората, имащи достъп чрез мобилни устройства, само до тези които изпълняват определени функции и/или които се ползват с най-голямо доверие;
- лимитиране на вида на устройствата, с които е разрешено свързване към мрежата, например лаптопите са разрешени, но смартфоните и таблетите - не;
- лимитиране на устройствата, на които е разрешено свързана към корпоративната мрежа само до тези, които са получили одобрение от ИТ отдела;
- само мобилните устройства, собственост на компанията, имат разрешение за достъп до корпоративната мрежа; подход, осигуряващ висока степен на сигурност, но изискващ от организацията да инвестира в мобилни устройства.

Споразумение за използване на собствени мобилни устройства от крайните потребители –

(BYOD End User Agreement)

Организациите трябва да приемат и сключат официално споразумение със своите служители при използване на лични устройства за достъп и съхранение на данни на организацията. То може да включва следното примерно съдържание:

1. Служителят носи отговорност за сигурното съхранение на информацията на организацията на устройството
2. Служителят е отговорен за покриване на всички разходи за устройството, включително в случаите, когато е използвано за нуждите на организацията.

3. Служителят се задължава да използва силни пароли за устройството, като може да се изисква допълнително криптиране на устройството.
4. Служителят е съгласен на устройството да бъде инсталиран софтуер за дистанционно управление, който позволява изтриване на данните или заключване на устройството.
5. Служителят се задължава да съобщи незабавно на работодателя си, ако устройството бъде загубено.
6. Изтриването на устройството може да доведе до изтриване на лична информация (напр. снимки); служителят е уведомен за това и приема че е негова отговорността за създаване на резервни копия на всичката лична информация, намираща се на устройството;

7. Служителят е съгласен, в случай на разследване за инциденти с данните, устройството да бъде анализирано от работодателя или разследващи служби, което може да доведе до разкриване на лични данни;
8. Устройството не може да бъде използвано за съхранение на следните видове данни (*работодателят прилага списък на чувствителната информация, която не може да бъде съхранявана на устройството)*;
9. Устройството не може да бъде използвано за изпращане на информация на организацията до други устройства или системи;
10. Служителят е съгласен да изтрие всички данни на организацията от устройството, преди да го предаде за унищожаване.

Заключение

Множество анализи и оценки на експерти и бизнес лидери показват, че работата от разстояние, в частност от вкъщи, се възприема много позитивно както от организациите, така и от техните служители, тъй като осигурява гъвкавост при съчетание на служебните и личните ангажименти.

Затова е сигурно, че за в бъдеще този модел ще получава все по-широко и масово приложение, което неминуемо ще доведе до нарастване на заплахите и рисковете за информационната сигурност.

Това ще изисква от организациите по-голямо внимание, ресурси и усилия по отношение на разработването на политики и стратегии и на прилагането на мерки за информационна и кибер сигурност, които трябва да осигурят непрекъснатост на бизнес процесите.

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!