48. Сигурност на информационни системи – общи понятия и класификация

Сигурността на една информационна система се обуславя от хардуера, софтуера, услугите и процедури, проектирани да защитят мрежите на дадена организация, приложенията и наборите данни, поддържани и функциониращи в нея. Всяко действие, което би нарушило поверителността, цялостта и наличността им е заплаха. Заплахите биват физически и по електронен път и са резултат от невнимание или злонамерена атака.

Макар и да не съществува информационна система, която да е на 100% защитена, съществуват критерии за определяне нивото на сигурност. Сигурността на информационните системи се определя от следните критерии: ефективност, целесъобразност (ефикасност), конфиденциалност (поверителност), интегративност (цялост), достъп (достъпност), съвместимост (compliance), надеждност. На базата на тези критерии могат да се поставят следните оценки на рисковете: стратегически риск, риск за сигурността, правен риск (в законодателно отношение), репутационен риск. Стратегическия риск има за цел да даде стратегическа оценка и анализ на риска, както и да дефинира цялостния процес за управление на аутсорсинг отношения с трети лица доставчици. При правният риск опазването на личните данни е сериозен проблем, като освен това има стремеж за конфиденциалност (правила за конфиденциалност) - съответствие на закони, правила и отчети на регулаторните органи. Регулаторните органи следят за тези правила. Рискът за сигурността се контролира чрез потребителска сигурност, аутентизация/администриране на достъпа на потребителите, дозирано достъпване на информацията, защитеност от външни и вътрешни атаки, конфиденциалност на транзакциите.
Ползват се и практики за сигурност на клиентите, които са внедрени и представляват съвети към клиента, предоставяне на информация за предотвратяване на риска. Автентикация на клиентите означава еднозначно разпознаване.

Системите за сигурност трябва да покриват пет ключови цели. Това са автентикация (упълномощяване), контрол на достъпа, интегритет на данните, non-repudation, конфиденциалност на данните. Автентификацията/упълномощяването предпазва системата от достъп на неоторизирани потребители, които целят злоупотреба с данните или изваждане "извън строя" на операционната система. Контрол на достъпа представлява защита на активите от неправомерно използване. Решенията, реализиращи тази цел, решават проблемите с конфиденциалността и интегритета на данните. Интегритетът на данните цели защита от заплахи, свързани с повреда или измама с данните. Non-repudation означава получателят и изпращачът да не могат да се отрекат от данните. Конфиденциалност на данните включва защита срещу неоторизирано разкритие на информация.