Насоки за следење и управување на инциденти поврзани со информациска безбедност

1. Органите организираат и воспоставуваат центар за управување со инциденти поврзани со информацискатa безбедност (CERT тим) и развиваат формални процедури за следење и управување со безбедносни инциденти.

2. Безбедносен инцидент претставува настан кој предизвикува или може да предизвика нарушување на интегритетот, достапноста и доверливоста на информациските ресурси.

3. Целта на процесот за управување со безбедносни инциденти е ефикасно и рентабилно обновување на нормалните операции што е можно побрзо, со најмалку можно негативно влијание врз деловниот процес и целите на институцијата.

4. Критичен елемент од управувањето со безбедносниот инцидентот е обновување на функциите на системот.

5. Процесот за управување со информациско - безбедносни инциденти треба да ги вклучува следните елементи:
   а) откривање на инцидентот;
   б) единствена точка за пријавување;
   в) евидентирање;
   г) доделување на приоритет на инцидентот и негова класификација;
   д) проценка на настанот/инцидентот и одлука за начинот на справување со него;
   ѓ) дефинирање на прво ниво за решавање на инциденти и услови за пренасочување на друго повисоко ниво;
   е) обновување;
   ж) верификација и затворање на инцидентот;
   з) идентификација на потребни подобрувања на процедурите за справување со безбедносни инциденти;
   ѕ) следење на инцидентите и управување со нивниот животен циклус.

6. Тимот за управување со безбедносни инциденти подготвува Правила за управување со безбедносни инциденти кои треба да ги содржат следните елементи:
   а) список на идентификувани важни функции на системот и приоритетите за обновување на функционалностите на системот;

б) список на идентификувани ресурси кои се неопходни за исполнување на критично важните функции;
в) список на можните инциденти со веројатности за нивно појавување, произлегувајќи од оценките на ризикот;
г) разработени стратегии за обновување на функционалноста на системот;
д) дефинирани мерки за реализација на стратегиите.

7. Правилата за заштита од инциденти, кои произлегуваат од оценката на ризикот, треба јасно да ги идентификуваат ресурсите кои е потребно да се резервираат за обновување на функциите на системот.

8. Основните правила за заштита од точка 7 се:
   а) паралелно запишување или огледална репликација на чуваните податоци (технологии "Disk Mirroring" или "RAID" - "Redundant Array of Independent Drives");
   б) создавање на центар за обновување по инциденти (т.н. "Disaster Recovery Center"), во кој што се извршува постојано архивско чување ("back-up") на информациите од системот;
   в) создавање на резервен центар, во кој што се одржува реплицирана состојба на критичните оперативни функции на примарниот систем, кој ќе биде во состојба да ја преземе функционалноста доколку се случи пад на системот.

   Органите зависно од потребите може да користат и комбинација од овие правила, со исклучок на правилото утврдено во алинејата 2 кое е задолжително.

9. Активностите за управување со безбедносни инциденти треба да вклучуваат мерки кои треба да се спроведат по обновувањето со цел избегнување на слични инциденти во иднина. Тоа треба да бидат мерки за:
   а) зголемување на нивото на контрола на пристап;
   б) промена на конфигурациите на зоните за безбедност;
   в) измена на режимот на физички пристап;
   г) инсталирање на дополнителни модули за заштита на софтверот; и
   д) други контроли и механизми со кои се поправаат воочените недостатоци.

10. При евидентирањето на настаните и инцидентите треба да се создаваат и чуваат најмалку следните записи:
    а) датум и време на случување на настанот;
    б) единствен идентификатор на корисникот;
    в) тип на настанот;
    г) резултат од настанот;
    д) извор на настанот;

е) список на засегнатите објекти;
ж) опис на измените во системот кои произлегуваат од настанот.