ИНФОРМАЦИОННО ОБСЛУЖВАНЕ

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, факс: 02/ 943 66 07
office@is-bg.net www.is-bg.net
ЕИК: 831641791

Предоставяне на удостоверителни услуги от "Информационно обслужване" АД

Процедури за сигурност

Версия: 1.5
Дата на публикуване: 11.07.2011 г.

I. ОБЩИ РАЗПОРЕДБИ

ПРЕДМЕТ

Чл. 1

/1/ Настоящите "Процедури за сигурност" уреждат изискванията за информационна сигурност към дейността на "Информационно обслужване" АД като доставчик на удостоверителни услуги /наричано по-нататък за краткост "доставчик"/.

/2/ “Процедури за сигурност" съответства на общоприетите международни стандарти за информационна сигурност, включително стандартите ISO 27001:2005, Common Criteria Level 4 (на процедурно и практическо ниво) ANS X9.79, на изискванията за сигурност към доставчиците на квалифицирани сертификати (Qualified Certificate Providers), както и на разпоредбите на българското законодателство.

/3/ "Процедури за сигурност" дефинира следните мерки, в съответствие на чл.34 ал.1 и ал.2 от Наредбата за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и за изискванията при предоставяне на удостоверителни услуги:

1. управленски мерки за сигурност;
2. мерки за информационна сигурност;
3. разполагаеми средства и застраховка;
4. изисквания за надеждност на персонала;
5. мерки за осигуряване на защита и ограничаване на достъпа до отделни устройства и помещения;
6. мерки за осигуряване на защита срещу непозволен достъп до информационните системи;
7. мерки за осигуряване на защита срещу непозволени промени.

ЦЕЛ

Чл. 2 Целта на "Процедури за сигурност" е:

1. дефиниране на рамката за управление и поддръжка на информационната сигурност;
2. определяне на задълженията и отговорностите на ръководството и служителите на Доставчика при спазване на предвидените изисквания за информационна сигурност.

II. УПГАВЛЕНСКИ МЕРКИ ЗА СИГУРНОСТ

ОПРЕДЕЛЕНИЕ

Чл. 3 Управленските мерки по сигурност целят да контролират достъпа до информационните системи на Доставчика по такъв начин, че само оторизирани лица да имат достъп и включват изисквания относно:

1. анализ на риска и заплахите за сигурността;
2. идентификация и автентификация;
3. одит и отчетност;
4. застраховка и постоянно действаща защита;
5. управление на ключовете;
6. разполагаеми средства.

АНАЛИЗ НА РИСКА И ЗАПЛАХИТЕ

Чл. 4

/1/ Доставчикът въвежда мерки за контрол, базирани на анализ на риска и заплахите за сигурността. Детайлният контрол се определя от BS7799, Common Criteria Security Functions, QCP CA management and operation control и X9.79 CA environmental controls.

/2/ По отношение на своята дейност, Доставчикът идентифицира следните главни рискове, свързани с:

1. проверка на идентичността на заявителя на сертификат;
2. съдържание на сертификата;
3. създаване, разпространяване и приемане на сертификат;
4. управление на сертификатите:
   4.1. разкриване на информация за клиентите;
   4.2. предлаганите услуги и поддръжка на абонатите;
   4.3. временно спиране и прекратяване на сертификатите;
   4.4. обработка на заявки на Доверяващата се страна;
   4.5. прекратяване на сертификат.

/3/ Доставчикът дефинира мерки и изисквания, които целят да се изключат, избегнат, намалят и ограничат щетите от реализиране на главните рискове.

ИДЕНТИФИКАЦИЯ И АВТЕНТИФИКАЦИЯ

Чл. 5

/1/ Идентификацията и автентификацията включват разпознаване на обект (например, потребител, устройство или система) и проверяване на идентичността на този обект. Изискванията за идентификация и автентификация се определят за информационната система като цяло.

/2/ Всеки отделен обект следва да бъде идентифициран по такъв начин, че всеки достъп до информационната система да бъде осъществен на базата на това кой има достъп до информацията и с какви

класове информация той има право да работи.

ОДИТ И ОТЧЕТНОСТ

Чл. 6 Одитът на информационните системи включва хронологично записване на събития, които са се случили в системата с цел да може да бъде извършено възстановяване и проверка на последователността от събития и/или промените в дадено събитие. Информацията от одита се съхранява и защитава, така че действията, засягащи сигурността да могат да бъдат проследени до отговорната страна.

ГАРАНЦИИ

Чл. 7 Хардуерните и софтуерните механизми е необходимо да бъдат оценени поотделно, за да се осигурят достатъчни гаранции, че към системата се прилагат изискванията за сигурност и мерките за контрол, посочени в документа "Процедури за сигурност".

ПОСТОЯННА ЗАЩИТА

Чл. 8 Механизмите, които се ползват за прилагане на тези основни изисквания, трябва да бъдат постоянно защитени срещу фалшифициране и/или неоторизирани промени. Освен това, данните трябва да бъдат защитени, когато се предават по мрежата или други медии.

УПРАВЛЕНИЕ НА КЛЮЧОВЕТЕ

Чл. 9

/1/ Криптографските ключове се използват от Доставчика за:

1. гарантиране целостта на съобщенията изпратени по мрежи, които не са защитени;
2. автентификация на потребителите;
3. защита на конфиденциалността на лична информация;
4. защита на съхранена поверителна информация, като например от записи от проведени ревизии.

/2/ След генерирането, ключовете се съхраняват, активират, деактивират и унищожават, които функции трябва да бъдат извършвани по сигурен начин като се използват подходящи контроли.

/3/ Доставчикът предприема мерки, които гарантират, че ключовата му двойка е генерирана по защитен и сигурен начин. Тези мерки включват:

1. при генерацията на ключовата двойка се използва криптографско хардуерно устройство, отговарящо на FIPS-140 Level 3;
2. при генерацията на ключовата двойка се прилага многофакторен контрол за достъпа;
3. само упълномощен персонал участва при генерацията на ключовата двойка;
4. дължината на ключа е в съответствие с Наредбата за изискванията към алгоритмите за създаване и проверка на квалифициран електронен

подпис;
5. алгоритмите са в съответствие с Наредбата за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис.

/4/ Доставчикът предприема мерки, които гарантират, че частният му ключ е със запазен интегритет и конфиденциалност. Тези мерки включват:

1. при съхраняване на частния ключ на Доставчика се използва криптографско хардуерно устройство, отговарящо на FIPS-140 Level 3+;
2. частният ключ на Доставчика не се архивира в явен вид;
3. при необходимост от възстановяване на частния ключ, Доставчикът използва многофакторен контрол или поделяне на части;
4. само упълномощен персонал участва във възстановяването на частния ключ.

/5/ Доставчикът предприема мерки, които гарантират, че публичният му ключ е със запазен интегритет и автентичност. Тези мерки включват:

1. публичният ключ на Доставчика се разпространява като част от сертификат;
2. достъпът до публичния ключ се осигурява посредством:
   2.1. защитена връзка към сайта на Доставчика;
   2.2. записване на сертификата с публичния ключ върху носител за еднократен запис, без възможност за добавяне на нови записи;

3. публичният ключ се променя през определен период от време;
4. ако Доставчикът е регистриран, то той задължително предоставя сертификата със своя публичен ключ, на Комисията за регулиране на съобщенията за публикуване.

/6/ Частният ключ на Доставчика не се предоставя за съхранение на трета страна.

/7/ Частният ключ на Доставчика се използва само за подписване на издадени от него сертификати.

/8/ Доставчикът предприема мерки, които гарантират, че частният му ключ е унищожен напълно в края на жизнения му цикъл. Тези мерки включват:

1. унищожават се всички части, фрагменти или други данни за възстановяване на частния ключ;
2. изтриват се ключовете, съдържащи се в криптографските хардуерни модули;
3. криптографските модули са защитени срещу кражба и опит за отваряне;
4. само упълномощен персонал участва в унищожаването на частния ключ.

/9/ Доставчикът издава персонални сертификати само върху смарт карта.

/10/ Доставчикът предприема мерки, които гарантират, че данните за активиране и смарт картата са разделени по място и време. Тези мерки включват:

1. абонатът получава смарт картата си веднага след издаването на сертификата;
2. данните за активиране се доставят по алтернативен канал.

III.МЕРКИ ЗА ИНФОРМАЦИОННА СИГУРНОСТ

ПРЕДМЕТ

Чл. 10 Мерките за информационна сигурност се състоят в създаване на:

1. документ "Процедури за сигурност";
2. организация по управление на сигурността;
3. осигуряване на възможност за извършване на одит на информационната сигурност от независим одитор;
4. ограничения за достъп на трети лица до системите за обработка на информацията;
5. класифициране на информацията за активите на Доставчика.

"ПРОЦЕДУРИ ЗА СИГУРНОСТ"

Чл. 11

/1/ Документът "Процедури за сигурност", се изготвя от началник отдел и главният администратор по информационна сигурност, утвърждава се от изпълнителния директор на "Информационно обслужване" АД и се довежда до знанието на всички служители на Доставчика.

/2/ Документът "Процедури за сигурност" се представя в Комисията за регулиране на съобщенията за одобрение.

ПРЕДОСТАВЯНЕ НА УДОСТОВЕРЕНИЕТО ЗА ЕЛЕКТРОНЕН ПОДПИС

Чл. 12

/1/ При регистрацията си, доставчикът предоставя на Комисията за регулиране на съобщенията своето удостоверение за усъвършенстван електронен подпис, съдържащо публичния му ключ.

/2/ В случай на компрометиране сигурността на частния си ключ, доставчикът уведомява Комисията за регулиране на съобщенията, след което й предоставя удостоверението за своя нов публичен ключ.

НЕЗАВИСИМ ОДИТ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Чл. 13 Доставчикът осигурява възможност за извършване на одит на "Процедури за сигурност" от независим, упълномощен за целта одитор.

ОГРАНИЧЕНИЯ ЗА ДОСТЪП НА ТРЕТИ ЛИЦА ДО СИСТЕМИТЕ ЗА ОБРАБОТКА НА ИНФОРМАЦИЯТА

Чл. 14 Контролът за достъп на трети лица до системите за обработка на информацията включва:

1. контрол на физическия достъп до помещенията;
2. регистриране на посетителите;
3. наблюдаване на помещенията чрез TV система за наблюдение;
4. определяне на зони "Забранено влизането" за посетители в периметрите със специализиран достъп;
5. определяне на зони "Само с придружител" за посетители в периметри с ограничен достъп;
6. подписване от третите лица на декларации за конфиденциалност и неразгласяване на информация.

КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

Чл. 15

/1/ Информацията се класифицира и обозначава като:

1. секретна;
2. поверителна;
3. служебна;
4. публична.

/2/ Доставчикът определя свои собствени процедури за обработване и управление на информация в съответствие с класификационната схема по ал.1, които включват документиране на информацията в описи и бази данни, а също осъвременяване или изтриване на информация при необходимост.

/3/ Терминът "чувствителна информация" се използва за обозначаване на информация на доставчика, която има поверителен и/или секретен характер.

IV. ИЗИСКВАНИЯ ЗА НАДЕЖДНОСТ НА ПЕРСОНАЛА

ДЛЪЖНОСТНИ ХАРАКТЕРИСТИКИ

Чл. 16 Доставчикът включва в длъжностните характеристики на своите служители задължения и отговорности, свързани с осигуряване на сигурността.

КОНТРОЛ НА ПЕРСОНАЛА

Чл. 17 Доставчикът извършва проверка на самоличността и надеждността на служителите си чрез изискване за представяне на:

1. документи в оригинал, изисквани за заемане на съответната длъжност;
2. официални документи, за доказване на самоличност;
3. свидетелства за съдимост.

ДЕКЛАРАЦИИ ЗА КОНФИДЕНЦИАЛНОСТ

Чл. 18 Служителите на Доставчика подписват декларации за конфиденциалност, което задължение е едно от условията за сключването на трудови договори с тях.

ПОДГОТОВКА И ОБУЧЕНИЕ ПО ИНФОРМАЦИОННА СИГУРНОСТ

Чл. 19 Служителите на Доставчика се обучават и периодично усъвършенстват познанията си относно информационната сигурност.

РЕАКЦИЯ ПРИ НАРУШЕНИЯ НА СИГУРНОСТТА

Чл. 20

/1/ Нарушенията на сигурността на информационните системи се докладват незабавно след откриването им на ръководителя на звеното, който отговаря за тяхното отстраняване.

/2/ Служителите на Доставчика имат право да правят предложения и да докладват за допускани нарушения относно сигурността.

/3/ Неизправности в софтуера се докладват на оперативния ръководител или на определен администратор.

/4/ Доставчикът назначава служител/и, които периодично анализират нарушенията на сигурността, с цел да се посочат потенциалните рискове и разходите за покриването им.

/5/ Мерките и процедурите за действие при възникване на технически проблеми във връзка със сигурността са посочени в документа "План за действие при извънредни обстоятелства и възстановяване след бедствия".

ДИСЦИПЛИНАРНА ОТГОВОРНОСТ

Чл. 21 Служителите на Доставчика носят дисциплинарна отговорност по Кодекса на труда при нарушаване на "Процедури за сигурност".

V. МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА И ОГРАНИЧАВАНЕ НА ДОСТЪПА ДО ОТДЕЛНИ УСТРОЙСТВА И ПОМЕЩЕНИЯ

ПЕРИМЕТРИ НА ФИЗИЧЕСКА ЗАЩИТА

Чл. 22

/1/ Доставчикът въвежда периметри на сигурност за Удостоверяващия орган с цел защита на зоните, в които са разположени системите за обработка на информация.

/2/ Определят се четири (4) нива на защитени зони:

1. Специализиран достъп (трезор - **Периметър 1**);
2. Ограничен достъп (извън трезора - **Периметър 2**);
3. Контролиран достъп (помещения за допускане на служители, които имат право на достъп до вътрешна информация - **Периметър 3**);
4. Наблюдаван достъп (помещения за другия персонал, коридори и общ достъп до помещенията - **Периметър 4**).

КОНТРОЛ НА ФИЗИЧЕСКИЯ ДОСТЪП

Чл. 23

/1/ Защитените зони се обезопасяват чрез подходящ контрол на входовете, за да се гарантира, че само оторизирани служители на Доставчика имат право на достъп.

/2/ Контролът по ал.1 включва:

1. записване на всички посетители;
2. предварително обявяване на посещения от външни лица, помощен персонал, и др.;
3. телевизионна система за наблюдение (CCTV);
4. влизане само с придружител до зоните с ограничен и специализиран достъп.

ОБЕЗОПАСЯВАНЕ НА ПОМЕЩЕНИЯТА И УСТРОЙСТВАТА

Чл. 24 Доставчикът внедрява механизми за сигурност, които защитават физически помещенията и устройствата със специални изисквания за безопасност, които включват:

1. 24 часово наблюдение на устройствата;
2. системи за откриване на проникване;
3. телевизионна система за наблюдение (ССПУ);
4. контрол на служителите;
5. наблюдение на мрежата;
6. незабавни действия при нарушения.

ДЕЙНОСТИ В ЗАЩИТЕНИТЕ ЗОНИ

Чл. 25 Доставчикът прилага допълнителни контроли и указания за своите

служители, работещи в защитените зони, които включват:

1. двуфакторна система за контрол на достъпа;
2. предупреждения за действието на телевизионна система за наблюдение;
3. предупреждения за наблюдение на системите;
4. използване на криптиращи системи, допълнителни криптографски модули за пароли и др.

ИЗОЛИРАНИ ЗОНИ ЗА ДОСТАВКИ

Чл. 26 Доставчикът приема доставките на стоки и оборудване в помещения, които физически са отделени от защитените зони. Доставките се контролират по всяко време, като транспортирането им до защитените помещения се извършва изключително и само под наблюдението на служителите на Доставчика.

РАЗПОЛОЖЕНИЕ НА ОБОРУДВАНЕТО

Чл. 27 Оборудването на Доставчика трябва да бъде разположено или подсигурено по такъв начин, че да бъдат намалени рисковете от природни бедствия и възможностите за неоторизиран достъп.

ЕЛЕКТРОЗАХРАНВАНЕ В ЗАЩИТЕНИТЕ ЗОНИ

Чл. 28 Доставчикът осигурява автономно функциониране на електрозахранването в защитените зони чрез използване и на вътрешни възможности за захранване, като по този начин осигурява защита на оборудването от прекъсване или повреди в електрозахранването.

ЗАЩИТА НА КАБЕЛНИТЕ СИСТЕМИ

Чл. 29 Доставчикът осигурява защита срещу прекъсвания или повреди в електрическите и телекомуникационните кабелни системи, които пренасят данни или поддържат информационни услуги.

ПОДДРЪЖКА НА ОБОРУДВАНЕТО

Чл. 30 Посредством договорите за гаранционна и извънгаранционна поддръжка на оборудването, доставчикът осигурява високо ниво на поддръжка на оборудването, в съответствие с инструкциите на производителя.

ЗАЩИТА НА ОБОРУДВАНЕТО ИЗВЪН ПОМЕЩЕНИЯТА

Чл. 31 Доставчикът използва процедури за сигурност и контроли, включително подписване на декларация за конфиденциалност и опис на изнесеното и на полученото оборудване, за да го защити при използване извън неговите помещения.

ГАРАНЦИИ ПРИ ИЗВАЖДАНЕ ОТ УПОТРЕБА И ПРИ ПОВТОРНО ИЗПОЛЗВАНЕ НА ОБОРУДВАНЕ

Чл. 32 Доставчикът осигурява изтриване на информацията от оборудването с

изключение на криптографските ключове и други секретни материали, преди същото да бъде извадено от употреба или повторно използвано. За изтриване на секретни материали, доставчикът назначава специална комисия.

ЗАЩИТА НА СЕКРЕТНИТЕ МАТЕРИАЛИ

Чл. 33 Доставчикът осигурява условия за недопускане на физически достъп на неоторизирани лица до секретни материали.

ПРЕМЕСТВАНЕ НА ОБОРУДВАНЕ ИЛИ СОФТУЕР

Чл. 34 Оборудване или софтуер, принадлежащи на Доставчика не могат да бъдат премествани без разрешение на отговорните лица.

VI. МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА СРЕЩУ НЕПОЗВОЛЕН ДОСТЪП ДО ИНФОРМАЦИОННИТЕ СИСТЕМИ

ОПЕРАТИВНИ ПРОЦЕДУРИ И ОТГОВОРНОСТИ

Чл. 35

/1/ Доставчикът осигурява правилното и сигурно опериране на системите, обработващи информация.

/2/ Всички промени и обновявания на системите по т.1 се контролират и документират.

ПРОЦЕДУРИ ЗА УПРАВЛЕНИЕ ПРИ НАРУШЕНИЯ

Чл. 36 Доставчикът определя отговорностите и процедурите за управление при нарушения на сигурността, които включват:

1. разпределяне на задачите;
2. вписване на задачите по т.1 в длъжностните характеристики на служителите;
3. определяне на степента на заплаха;
4. определяне на нивата за докладване при констатиране на нарушения.

РАЗДЕЛЯНЕ НА СИСТЕМИТЕ ЗА РАЗРАБОТКА ОТ ОПЕРАТИВНИТЕ СИСТЕМИ

Чл. 37 Системите за разработка и тестване на Доставчика са функционално и физически разделени от оперативните системи.

ПЛАНИРАНЕ И ПРИЕМАНЕ НА НОВИ ИНФОРМАЦИОННИ СИСТЕМИ

Чл. 38

/1/ Преди въвеждане на нови информационни системи доставчикът проучва необходимите капацитети, за да гарантира, че са в наличност достатъчно мощности за обработка и съхранение.

/2/ Нови информационни системи, обновени или нови техни версии се тестват преди да бъдат приети.

ЗАЩИТА НА СОФТУЕРА

Чл. 39 Софтуерът се контролира и тества преди неговото използване.

АРХИВИРАНЕ НА ИНФОРМАЦИЯ

Чл. 40

/1/ Доставчикът осигурява периодичното изготвяне на архивни копия на важната информация и софтуер и съхранява допълнителни копия на системни операции, журнални файлове, наблюдения с камери и определени

функции, свързани с издаването, управлението, спирането и прекратяването на удостоверенията за електронен подпис.

/2/ Доставчикът поддържа синхронни копия на:

1. оперативните системи по издаване и управление на сертификати;
2. хранилищата на сертификати;
3. своя сайт.

/3/ Доставчикът архивира ежедневно цялата информация от:

1. оперативните системи по издаване и управление на сертификати;
2. хранилищата на сертификати;
3. своя сайт.

/4/ архивите се съхраняват в защитено помещение в огнеупорна каса за период от един месец.

ЖУРНАЛИ НА ОПЕРАТОРИТЕ

Чл. 41

/1/ Поддържат се журнали за действията на операторите на Доставчика.

/2/ Доставчикът осигурява контрол върху журналите, докладване на записаните грешки и предприемане действия за коригирането им.

/3/ Всеки запис в журналите включва следните елементи:

1. дата и време на записа;
2. идентификатор на събитието;
3. резултат от събитие;
4. идентификатор на източника на записа;
5. идентичността на осъществилия запис.

/4/ събитията които се записват са:

1. генерация на сертификат;
2. генерация на CRL;
3. всички служебни съобщения.

/5/ Записите в журналите се генерират автоматично или ръчно.

/6/ Журналите се съхраняват в електронен формат или в хартиен формат.

/7/ Гарантира се интегритета на записите.

/8/ Само упълномощен персонал има достъп до журналите.

МРЕЖОВИ КОНТРОЛИ

Чл. 42 Доставчикът въвежда серия от контроли за постигане и поддържане на безопасност в мрежите, според документа "Процедури за сигурност".

СИГУРНОСТ ПРИ РАБОТА С КОМПЮТЪРНИ НОСИТЕЛИ

Чл. 43

/1/ Доставчикът осигурява работата със сменяеми компютърни носители /ленти, дискове, касети и отпечатани доклади/ чрез:

1. точно означаване на статуса им;
2. съхранението им на недостъпни места;
3. записи на входящи и изходящи материали при съхранение в архива.

/2/ Въвеждат се мерки, които регламентират унищожаване на носители по ал.1, след като повече не са необходими, които включват:

1. използване на средства за сигурно унищожаване на данни на дисковете;
2. нарязване на отпечатаните материали и ленти.

ПРОЦЕДУРИ ЗА РАБОТА С ПОВЕРИТЕЛНАТА ИНФОРМАЦИЯ И СЪС СИСТЕМНА ДОКУМЕНТАЦИЯ

Чл. 44 Доставчикът разработва процедури за работа на служителите си с поверителна информация и със системна документация.

ЗАЩИТА ПРИ ОБМЕН НА ИНФОРМАЦИЯ И СОФТУЕР

Чл. 45

/1/ С цел да предотврати загуба или промяна на информация, доставчикът осигурява защита на:

1. носителите на информация;
2. електронните търговски транзакции на неговия публичен уеб сайт;
3. ползването на гласови, факс и видео устройства за комуникация.
4. работата с електронна поща.

/2/ Мерките по т.4 включват и обучение на служителите на Доставчика за рисковете при използване на електронна поща и използването на подходяща технология за защита.

/3/ Доставчикът предприема мерки за гарантиране целостността и конфиденциалността на информацията през целия цикъл на нейното създаване, обработка, съхранение и унищожаване. Тези мерки включват:

1. чувствителната информацията се обменя в криптиран вид;
2. при предаване на секретна информация се изисква изрично писмено разрешение;
3. забранява се предаване на чувствителна информация по открити средства за комуникация, като телефон, факс;
4. съобщенията по електронната поща, със служебен характер задължително се подписват;
5. забранява се копиране на чувствителна информация от един носител на друг без изрично писмено разпореждане;
6. при унищожаване на чувствителна информация се унищожават всички копия от тази информация;
7. Доставчикът води журнал за чувствителната информация в който се отразява кой, кога и до каква информация е имал достъп и къде се намира тя в момента.

УПРАВЛЕНИЕ НА ДОСТЪПА НА ПОТРЕБИТЕЛИТЕ ДО СИСТЕМИТЕ

Чл. 46

/1/ Доставчикът въвежда процедура по регистрация и дерегистрация на потребителите, за да предостави достъп до всички многопотребителски информационни системи и услуги.

/2/ Доставчикът ограничава и контролира разпределението и ползването на потребителски привилегии.

/3/ Доставчикът извършва периодичен преглед на правата за достъп на потребителите.

КОНТРОЛ НА ДОСТЪПА ДО МРЕЖАТА

Чл. 47

/1/ Доставчикът осигурява на потребителите директен достъп до услугите само, ако специално са били оторизирани за употребата им.

/2/ Доставчикът осигурява контрол на:

1. трасето от потребителския терминал до компютърната услуга;
2. достъпът до диагностичните портове.

/3/ Предмет на автентификация са:

1. достъпът на отдалечени потребители;
2. връзките с отдалечените компютърни системи.

/4/ Информационните услуги, потребителите и информационните системи се разделят на групи при управление на мрежата.

/5/ Възможността за връзка на потребителите в мрежата се ограничава, в съответствие с процедурите за достъп на Доставчика.

/6/ Общите мрежи имат контроли на маршрутите, за да се гарантира, че компютърните връзки и информационните потоци не нарушават правилата за достъп до бизнес приложенията.

/7/ Доставчикът осигурява ясна дефиниция на всички атрибути на сигурността за всички мрежови услуги, ползвани от организацията.

/8/ При предоставяне на достъп до мрежата на Доставчика на външни лица отношенията се регламентират чрез:

1. договор за реда и начина за предоставяне на достъпа;
2. подписване на споразумение за неразкриване на информация;
3. подписване от служителите на външното лице на декларации за неразкриване на информация.

КОНТРОЛ НА ДОСТЪПА ЧРЕЗ ОПЕРАЦИОННИТЕ СИСТЕМИ

Чл. 48 Чл. 47. С цел осъществяване контрол на достъпа чрез операционните системи доставчикът:

1. използва за автоматичната идентификация терминал за автентифициране на връзките с определени места и преносимо оборудване;
2. използва сигурен log-он процес за достъп до информационните услуги;
3. въвежда уникален идентификатор (потребителско ID) за всички потребители, само и единствено за тяхна употреба, като по този начин действията могат да бъдат проследени до лицето, което е отговорно за тях;
4. въвежда системата за управление на паролите като средство, с което се гарантира качеството им;
5. ограничава и стриктно контролира употребата на системните програми;
6. осигурява "принудителни" аларми за защита на тези от потребителите, които могат да бъдат обект на атака;
7. осигурява изключване на терминалите на места с висок риск или системи, осигуряващи услуги с високо ниво на риск след определен

период от време, в който не са действали, за да бъде предотвратен достъпа на неоторизирани лица;
8. използва ограниченията на времето за връзка, за да бъде осигурена допълнителна защита на високо рисковите приложения.

КОНТРОЛ НА ДОСТЪПА НА НИВО ПРИЛОЖЕНИЕ

Чл. 49

/1/ Доставчикът ограничава достъпа до информацията и приложните системи с цел предотвратяване на неоторизиран достъп до информацията, която се обработва и съхранява в информационните системи.

/2/ Чувствителните системи се изолират от останалите системи с общо предназначение.

СИСТЕМА ЗА НАБЛЮДЕНИЕ НА ДОСТЪПА И ПОЛЗВАНЕТО НА ИНФОРМАЦИОННИТЕ РЕСУРСИ

Чл. 50 Доставчикът осигурява контрол на достъпа и ползването на информационните системи чрез:

1. съхраняване на записите за извършени ревизии и други свързани със сигурността събития;
2. внедряване на процедури за наблюдение на ползването на устройствата, обработващи информация;
3. синхронизиране на часовниците на компютрите за осигуряване на точно записване;
4. съхраняване на записи от телевизионно наблюдение на защитените помещения.

VII. МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА СРЕЩУ НЕПОЗВОЛЕНИ ПРОМЕНИ

ЗАЩИТА НА ПРИЛОЖНИТЕ СИСТЕМИ

Чл. 51 Доставчикът осигурява защита на приложните системи чрез:

1. проверка на верността и точността на данните, въвеждани в приложните системи;
2. внедряване на проверки за валидност на приложните системи;
3. използване на автентификацията на съобщения за приложения, при които има изисквания да бъде защитена целостта на съдържанието на съобщението;
4. осигуряване на защита срещу вируси, "троянски коне" и злонамерен софтуер;
5. проверка на изходните данни от приложните системи с цел правилната обработката на съхранената информация.

КРИПТОГРАФСКИ КОНТРОЛ

Чл. 52

/1/ Доставчикът внедрява правила за използване на криптографски контроли за защита на конфиденциалността, автентичността и целостта на информацията.

/2/ За поддържането на системата за управление на ключовете, базирана на приета система от стандарти, процедури и методи се използват подходящи криптографски техники.

/3/ Доставчикът използва криптомодули, сертифицирани по FIPS 140-1, ITSEC или други критерии, гарантиращи адекватно или по-високо ниво на сигурност за:

1. защита на частния си ключ и електронен подпис:
   1.1. StampIT Primary Root CA - криптомодули, сертифицирани по FIPS 140-2 Level 3;
   1.2. StampIT Qualified CA- криптомодули, сертифицирани по FIPS 140-2 Level 3;
2. защита на частния ключ и електронен подпис на лицата, осъществяващи достъп до информационните системи - криптомодули, сертифицирани по ITSEC level E4 high.

ЗАЩИТА НА СИСТЕМНИТЕ ФАЙЛОВЕ

Чл. 53 Доставчикът осигурява защита на системните файлове чрез осъществяване на контрол на:

1. внедряването на софтуер в оперативните системи;
2. системните тестови данни;
3. достъпа до библиотеки с програмни кодове.

ЗАЩИТА НА ПРОЦЕСИТЕ ПО РАЗРАБОТКА И ПОДДРЪЖКА НА ПРИЛОЖЕН

СОФТУЕР

Чл. 54 Доставчикът защитава от промени приложния софтуер при неговата разработка и поддръжка чрез:

1. осъществяване на контрол при въвеждането на промени;
2. проверка и тестване на приложните системи при промяна;
3. ограничаване на модификациите в софтуерните пакети.

ОСИГУРЯВАНЕ НА НЕПРЕКЪСВАЕМОСТ НА ДЕЙНОСТТА НА ДОСТАВЧИКА

Чл. 55

/1/ Доставчикът разработва плановете за поддръжка или възстановяване на непрекъсваемостта на дейността си.

/2/ Плановете се тестват редовно и подлежат на редовни прегледи, за да се гарантира, че са актуални и ефективни.

ДЕЙСТВИЯ ПРИ НАРУШЕНИЯ НА СИГУРНОСТТА НА КЛЮЧОВЕТЕ

Чл. 56

/1/ В случай на нарушения на сигурността на частния ключ на Удостоверяващия орган или при възникване на основателно съмнение за подобни нарушения, доставчикът може да прекрати действието и да преиздаде всички удостоверения за електронен подпис, които са били подписани с неговия частен ключ [ISO 15782-1].

/2/ Доставчикът въвежда процедури за защитено и автентифицирано прекратяване на удостоверенията за електронен подпис при възникване на необходимост от замяна на частния му ключ, които включват:

1. стария публичен ключ на Доставчика;
2. целия комплект от удостоверения за електронен подпис, издадени от Доставчика, базирани на компрометирания частен ключ;
3. всеки частен ключ на подчинени Удостоверяващи Органи и кореспондиращите им сертификати.

/3/ Процедурите за възстановяване използвани, в случай, че собствените частни ключове на Доставчика са компрометирани и публичният ключ на Удостоверяващият орган е прекратен, включват следното:

1. възстановяване на защитената обкръжаваща сред;
2. прекратяване на стария публичен ключ на Удостоверяващият орган;
3. предоставяне на новия публичен ключ на потребителите;
4. преиздаване на удостоверенията за електронен подпис на потребителите.

/4/ Доставчикът определя страните, които трябва да бъдат уведомени и действията, които трябва да бъдат извършени по отношение на системния софтуер и хардуер, симетричните и асиметричните ключове и създадените преди това подписи и данни.

ПРОВЕРКИ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

Чл. 57 Доставчикът осъществява периодични проверки на информационните системи за съответствие с настоящата "Процедури за сигурност".

АРХИВИРАНЕ НА ИНФОРМАЦИЯ

Чл. 58 Доставчикът осигурява конфиденциалност и цялост на текущите и архивираните данни, отнасящи се до всички видове удостоверения за електронен подпис.