Computer Security Incident Response Team

CSIRT НА ФИНКИ

Елаборат за формирање

Факултет за информатички науки и
компјутерско инженерство

Содржина

Вовед

Сведоци сме на фактот дека безбедносните закани се неразделен дел од нашата реалност и дека секој вмрежен систем може потенцијално да биде компромитиран за помалку од неколку минути што може да предизвика прекин на сервис (downtime), кражба на податоци, репликација на вируси, црви и тројанци преку интернет. Игнорирањето на безбедноста може да ја чини организацијата време, напор, продуктивност, а во некои случаеви може да има значајно финансиско влијание како и загуба на угледот.
Едена од основните форми на дејствување со цел превенирање, но и справување со ваков тип на проблеми е воспоставувањето на CSIRT кое да спречи настанување на многу проблеми, но исто така и брз одговор на инциденти доколку тие се случат.

Computer Security Incident Response Teams (CSIRTs) се одговорни за примање и разгледување на репорти за инциденти, како и да одговорат соодветно на нив.
Ваков тип на услуги обично се вршат за дефинирана група како корпорација, институција, образовна или владина мрежа, регион или држава. CSIRT услугите обично се делат на 3 категории:

- реактивна (reactive) – пр. справување со инцидент, сигнали за ранливост
- проактивна (proactive) – пр. откривање на упад, ревизија и ширење на информации
- управување со квалитет на безбедност (security quality managment) – пр. анализа на ризик, планирање на опоравување од катастрофа, како и едукација и тренинг.

CSIRT може да биде формален тим или ад-хок тим. Формален тим одговорот на ризици го врши како примарна работна функција, додека пак ад-хок тимот е заедно кога ќе се појави потреба односно кога ќе има инцидент со компјутерската безбедност.

Следново треба да биде дефинирано при воспоставување на CSIRT:

- мисија – какви задачи треба да се преземат?
- конституција – на кого треба да му се служи?
- организација – каде CSIRT се вклопува во целосната организациона структура?
- односи – со кого да се соработува и на кој да му се верува?

Треба да се истакне дека CSIRT е општо прифатен генерички термин за тимови кои се задолжени за справување и одговор на инциденти. Биле традиционално познати како Computer Emergency Response Teams (CERTs) и многу се служат се уште со овој термин.
Различните термини се менливи и не имплицираат на различни улоги, иако услугите кои ги нуди може да зависат од еден и друг тим.
Елаборатот е базиран на претходните искуства, најдобрите пракси во областа, реализираните проекти (ENCYSEC) како и дипломскиот труд на Деница Веселиновска под менторство на вонр. проф. д-р Анастас Мишев.

Дефиниции и објаснувања

Што претставува компјутерски безбедносен инцидент?

Секоја организација мора да дефинира што претставува компјутерски безбедносен инцидент за нивниот сајт. Примери за општи дефиниции за компјутерски безбедносен инцидент: секој реален или сомнителен несакан настан во врска со безбедноста на компјутерските системи или компјутерските мрежи, чинот на прекршување на експлицитни или имплицитни безбедносни полиси.
Инцидентите може да вклучат акции како: обид за (успешен или не) неовластен пристап до системот или неговите податоци, несакани нарушувања или одбивање на услугата (denial of service), неовластено користење на системот за процесирање или чување на податоци итн. Активностите преземени во рамки на компјутерски безбедносниот инцидент може да се дефинирани како мрежа или активности на домаќин (host) кои потенцијално се закануваат на безбедноста на компјутерските системи.

Што претставува справување со инцидент ?

Справување со инцидент вклучува три функции: пријавување на инцидентот, анализа на инцидентот и одговор на инцидентот.
Функцијата за пријавување на инцидентот му овозможува на CSIRT да служи како централна точка за контакт за пријавување на локалните проблеми. Ова овозможува сите репорти и активности за инцидентите да бидат собрани на едно место каде што информациите може да бидат разгледани и поврзани во рамки на мајчината организација. Ова претставува еден дел од функцијата за анализа на инцидентот. Другиот дел од оваа функција претставува преземање на подлабоко разгледување на репортот за инцидентот со цел да се утврди обемот, приоритетот и заканата заедно со истражување за можните одговори и ублажувања. Функциите за одговор на инцидентот може да бидат во различни форми. CSIRT може да испрати препораки како да се направи оporавување и спречување на понатамошни инциденти, па потоа системските и мрежните администратори да ги извршат тие задачи сами или CSIRT може сами да ги извршат задачите врз погодениот систем. Одговорот може да вклучува и размена на информации и научени лекции со други одговорни тимови и соодветни организации.
Овие функции за справување со инциденти се реактивни услуги кои CSIRT може да ги понуди.

Зошто на организацијата и треба CSIRT ?

Дури и најдобрите инфраструктури за безбедност на информации не може да гарантираат дека нема да се случат упади или други злонамерни акти. Кога ќе се случи компјутерски безбедносен инцидент од клучно значење е за една организација да има ефективен начин да се одговори.
Брзината со која една организација може да препознае, анализира и одговори на инцидент ќе ја ограничи штетата и ќе ја намали цената на трошоците за опоравување.

CSIRT може да биде во состојба да спроведе брза реакција и да спречи инцидент како и брзо опоравување. CSIRT може да има познавање со компромитирани системи и затоа да може лесно и брзо да координира опоравување како и да предложи стратегии за ублажување и одговор.
Односот со други CSIRT тимови и организации за безбедност може да олеснат споделување на стратегии за одговор и рани сигнали за потенцијални проблеми. Тие може да помогнат во идентификувањето на ранливите области на организацијата и во некои случаи да извршат проценка на ранливоста и откривање на инцидентот.
Тие може да го фокусираат вниманието на безбедноста и да обезбедат обука на членовите во организацијата со цел да се зголеми свесноста за безбедноста. CSIRT исто така може да обезбедат експертиза за се превентивност и да помогнат во намалувањето на идните закани.

Какви типови на CSIRT постојат ?

CSIRT доаѓаат во сите облици и големини и служат на различни конституции. Некои CSIRT нудат поддршка за цела земја, регион или конкретен универзитет или организација.
Некои општи категории на CSIRT, но не се ограничени:

- Внатрешни (internal) CSIRTs – обезбедуваат справување со инциденти на својата матична организација. Такво CSIRT може да биде на банка, производствена компанија, универзитет или федерална агенција.
- Национални (national) CSIRTs – обезбедуваат справување со инциденти на една држава (пр. Japan CERT Coordination Center, Singapore Computer Emergency Response Team)
- Координаторни центри (Coordination Centers) – го координираат и олеснуваат справувањето со инциденти на други CSIRTs (пр. CERT Coordination Center or the United States Computer Emergency Readiness Team)
- Центри за анализа (Analysis Centers) – се фокусираат на собирање податоци од различни извори со цел да се утврдат трендови и модели во активностите на инцидентот.
- Vendor Teams)– се справуваат со репорти за ранливости во нивниот софтверски или хардверски производ. Тие може да работат во рамките на една организација за да се утврди колку нивниот производ е ранлив и како да се развијат стратегии за санација.
- Incident Response Providers – нудат услуги за справување со инциденти со плаќање на други организации.

Колку чини да се создаде CSIRT ?

Цената за создавање на CSIRT зависи од бројот на ресурси и услуги кои треба да се обезбедат, административни трошоци за областа или организацијата, како и од структурата на CSIRT.

Колку вработени треба да има CSIRT ?

Различни CSIRT имаат различни нивоа на вработени во зависност од нивните средства, потреби и обемот на работа. Моделот кој работи за една организација може да е работи за друга. Големината на персоналот на CSIRT треба да биде врз основа на достапните ресурси и услугите кои се неопходни да ги обезбеди.

Кој работи во CSIRT ?

Најдобрите вработени во CSIRT имаат технички вештини како и комуникациски вештини. Персоналот во CSIRT треба да е посветен, иновативен, флексибилен и аналитички. Тие се решавачи на проблеми, добри комуникатори, и може да се справат со стресни ситуации. Една од најважните особини на член на тимот што треба да ја поседува е интегритетот.

Креирање на CSIRT

Држење на информациите од организацијата безбедни во денешната меѓусебно поврзана компјутерска околина е вистински предизвик кој станува се потежок со секој нов 'е' продукт. Повеќето организации сфаќаат дека нема едно решение за безбедноста на податоците и системите, наместо тоа се бара повеќеслојна стратегија за безбедност. Еден слој кои многу организации го вклучуваат во нивната стратегија денес е токму креирањето на CSIRT тимови.

Кога организациите почнуваат да градат свои можности за справување со инциденти, ти се обидуваат да утврдат кој е најдобра стратегија за поставување на структурата на право место.

Иако сите CSIRT се разликуваат во тоа како работат во зависност од расположливиот кадар, стручноста, буџетот и уникатните околности на секоја организација, сепак постојат некои основни практики кои се однесуваат на сите CSIRTs. Ние ќе разгледаме некои од овие практики кои се однесуваат на создавање на CSIRT, кои иако се претставени како чекори сепак не се секвенцијални и многу чекори може да се случуваат паралелно.

Чекорите се следни:

1. Обезбедување поддршка за управување (менаџмент) – оваа поддршка треба да се покаже на повеќе начини, вклучувајќи и обезбедување на ресурси, финансиски средства и време, едно лице или група од луѓе кои ќе бидат проект тим за имплементација на CSIRT. Исто така ова вклучува и вработените во организацијата да посветат време за учество во овој процес на планирање бидејќи нивниот придонес е од суштинско значење. Важно е да се поттикнат очекувањата и перцепциите за функциите и одговорностите на CSIRT – без оваа информација тимот може ќе биде изграден, но неговите услуги да не се соодветни или доволно разбрани од страна на организацијата. Заедно со поддршката на процесот за планирање и имплементирање на CSIRT, треба да се обезбеди поддршка за подолг рок бидејќи без оваа поддршка долгорочниот успех на CSIRT може да биде во опасност.

2. Одредување на CSIRT стратешки план за развој – во оваа фаза треба да се разгледаат повеќе прашања: како да се справиме со развојот на CSIRT? Кои административни проблеми треба да се решат? Дали имаме временски рамки – ограничувања, дали се реални и ако не се дали може да бидат променети? Дали има група за проектот и од каде доаѓаат членовите? Треба да бидеме сигурни дека сите заинтересирани страни се претставени. Како организацијата ќе се информира за CSIRT? Со еден допис од извршниот директор или друг менаџер на повисоко ниво во кој ќе се објави стартувањето на проектот и ќе се побара претставник за помош од сите засегнати страни е добар начин за започнување. Да му се овозможи на организацијата да знае за планирањето на CSIRT уште од самиот почеток на развој може да им помогне на вработените да се чувствуваат како дел од процесот на дизајн. Ако имате тим кој ќе работи на проектот како ќе

се снимаат и разменуваат информациите кои се собрани, особено ако тимот е географски разделен?

3. Собирање на релевантни информации – се собираат информации за одговорите на инцидентите како и услугите од кои организацијата има потреба. Се разгледуваат активностите за време на инцидентот кои се неодамна пријавени во рамки на организацијата. Ова ќе помогне во одредувањето на кои услуги CSIRT треба да ги понуди како и кои вештини и способности ќе бидат потребни за персоналот во CSIRT. На пр. ако организацијата е жртва на некој компјутерски вирус, ќе има потреба од вработен со искуство во таа област. Исто така ќе треба скенирање на вирусот, елиминација и постапка за обновување заедно со соодветни анти-вирус алатки. Потребно е да се идентификуваат кои информации ќе бидат потребни за да се имплементира CSIRT, исто така и од кого може да се добијат тие информации.

4. Дизајн на CSIRT визија – кога собирањето на информации ќе почне во прв ред да ги носи потребите од одговор на инцидентот и разбирањето на управувањето на CSIRT, ќе почне да се идентификуваат клучните компоненти на CSIRT. Ова овозможува да се дефинира дизајнот на визијата на CSIRT, цели и функции. Важно е да се постигне договор за дефиницијата и очекувањата од CSIRT. Главниот фокус на CSIRT е да се спречи и одговори на инциденти. Визијата за CSIRT мора да вклучува јасно објаснување каде функциите на CSIRT се вклопуваат во сегашната структура на организацијата и како CSIRT ќе се поврзе со организацијата. Визијата објаснува кои се предностите CSIRT што ги обезбедува, што носат процесите, кој процеси ги координира, и како ќе ги изведува акциите за одговор.

5. Разговор за CSIRT визијата – потребно е да се сподели визијата со тимот за управување, организацијата и сите други што треба да ги знаат и разбираат функциите на CSIRT. Потоа се прави корекција на визијата и планот од добиените одговори. Со споделување на визијата однапред може да се идентификуваат процесни или организациони проблеми пред самата имплементација. Тоа претставува начин луѓето да дознаат што се најавува и им дозволува да допринесат за имплементацијата на CSIRT. На овој начин може да се добијат информации кои се пропуштиле или не биле достапни во чекорот кога се собирале информациите. Се користат сите информации за да се направат финални измени во CSIRT организационата структура и процеси.

6. Започнување на имплементацијата на CSIRT – откако ќе се создаде визијата, се започнува со имплементација:
    - вработување и обучување на иницијален CSIRT персонал
    - купување на опрема и градење на мрежната инфраструктура за поддршка на тимот
    - развивање на почетниот сет полиси-политики и процедури на CSIRT за поддршка на услугите
    - дефинирање на спецификациите за изградба на систем за следење на инциденти

- развивање на упатства за пријавување на инциденти и форми за организацијата.

Главен ресурс потребен на организацијата е упатството за пријавување на инцидентите. Ова упатство дефинира како организацијата ќе комуницира со CSIRT, што претставува инцидент, каков тип на инциденти се пријавуваат, кој треба да пријави инцидент, зошто еден инцидент треба да се пријави, кој е процесот на пријавување на инцидент и процесот на одговор на инцидентот. Упатствата треба да бидат чисти и разбирливи со цел да му служат на организацијата. Процесот на пријавување на инцидент вклучува детален опис на механизмите за пријавување на извештај како и типот на информации што треба да се содржат во репортот. Процесот на одговарање на инциденти вклучува објаснување како CSIRT дава приоритет на инцидентот и како се справува со репортите.

7. Објавување на CSIRT – кога CSIRT ќе стапи на функција, треба да се претстави на организацијата. Најдобро е ако оваа објава дојде со информации за контакт и работно време како и упатството за пријавување на инцидент. Оваа информација може да се прошири преку едноставна брошура, флаер, посебна прослава, или мејл.
8. Оценка на ефикасноста на CSIRT – откако CSIRT ќе биде во функција некое време, управителите ќе сакаат да ја видат ефикасноста на тимот и резултатите, евалуација и подобрување на CSIRT и да се осигура дека тимот ги добива корисните информации од организацијата. CSIRT во соработка со менаџментот и организацијата треба да се обезбеди евалуација. Постојат различни начини за да се оцени ефективноста на CSIRT, некои од нив се: споредба со други CSIRT, општи дискусии со претставници на организацијата, доставување на евалуација до членови од организацијата, итн.

CSIRT услуги

Едно од основните прашања кои треба да се одговорат при креирање на CSIRT е одлуката какви услуги ќе им понуди CSIRT на своите корисници во организацијата. Овој процес значи именување и дефинирање на секоја понудена услуга, што не секогаш претставува лесна задача. Искуството покажало дека често има голема забуна во врска со имињата кои се користат за CSIRT услугите. Тука ќе претставиме листа на услуги и нивните дефиниции. CSIRT треба внимателно да ги одбере услугите кои ќе ги понуди. Изборот на услуги треба да ги исполнува бизнис целите на организацијата. Услугите кои треба реално и искрено да ги понудат бидејќи истите треба да ги реализираат. Подобро е да се понуди помал број добри услуги , отколку голем број лоши услуги. Со текот на времето како што CSIRT ќе ја добива довербата и почитта во организацијата, може да ги прошири своите услуги и персонал.

Категории на услуги

Постојат многу услуги кои CSIRT може да ги понуди. Секој CSIRT е различен и обезбедува различни услуги во зависност од мисијата, целта и организацијата.
Примарните CSIRT услугите може да бидат групирани во три категории:

1. Реактивни услуги – reactive service. Овие услуги се дизајнирани со цел да одговорат на некој настан или барање, како што е пријавување на компромитиран домаќин host, широко распространет малициозен код, софтверска ранливост, или нешто што е детектирано од страна на intrusion detection logging system. Овие услуги се основна компонента работата на CSIRT.
2. Проактивни услуги – proactive service. Овие услуги обезбедуваат помош и информација за да се подготви, заштити и обезбеди системот во организацијата во однос на напади, проблеми или настани. Перформансите на овие услуги директно ќе го намали бројот на инциденти во иднина.
3. Безбедносни услуги за управување со квалитет – Security quality managment services. Овие услуги ги подобруваат постоечките услуги кои се независни и одвоени од справувањето со инциденти и најчесто се изведуваат од други области во организацијата како што се ИТ и одели за обуки. Доколку CSIRT ги нуди овие услуги или помага околу нив тогаш тој може да помогне во подобрување на севкупната безбедност на организацијата и да ги идентификува ризиците, заканите како и системските слабости.

Како дополнителни активности на CSIRT можат да бидат истражувања во областа на компјутерската безбедност, организација на настани, предавања и конференции од областа на безбедноста, воспоставување соработка со сите други релевантни чинители во компјутерската безбедност и многу други.

Во таблата подолу се претставени кои услуги се нудат во соодветната категорија:

Reactive services	Proactive services	Security quality management services
Alerts and warnings	Announcements	Risk analysis
Incident handling	Technology watch	Business continuity and disaster recovery planning
Vulnerability handling	Security audits or assessments	Security consulting
Artifact handling	Security related information dissemination	Awareness building
	Development or security tools	Education/ training
	Intrusion detection services	Product evaluation or certification
	Configuration and maintenance of security tools, applications and infrastructures	

Креирање CSIRT на ФИНКИ

Следејќи ги претходно опишаните чекори, како и нивно дополнување заради прилагодување кон можностите и околината, следува предлог решение за тоа како да се креира CSIRT на ФИНКИ. Следниот обид ќе претставува преглед на акциите што треба да се преземат при креирање на CSIRT како и можните проблеми при неговата имплементација.

Чекорите за формирање на CSIRT на ФИНКИ:

1. Идентификување на 'засегнатите страни' (stakeholders) и учесниците.
   Засегнатите страни од нашиот тим може да ги поделиме во две поголеми групи. Едната група е групата на студентите на факултетот, а другата група е групата на вработените во факултетот. CSIRT треба да им служи на двете групи кои ги дефиниравме. Според моменталната организираност на факултетот вработени кои нудат услуги блиску до услугите на CSIRT се систем инженерите од КЦ, кои треба да бидат активно вклучени во идниот CSIRT. Особено внимание треба да се посвети на активно вклучување на студентите во работата и активностите на CSIRT на ФИНКИ, со оглед дека тие претставуваат доминантна група по својата бројност.
2. Обезбедување на поддршка и спонзорство.
   Потребно е да се обезбеди доволно време и ресурси кои на тимот ќе му бидат потребни за истражување и собирање на информациите. Иницијалната идеа при формирањето на сервисот е во него да бидат вклучени сите заинтересирани во рамките на своите можности и на доброволна основа. Во иднина, доколку CSIRT започне да нуди и сервиси кон други организации за кои ќе бара финансиски надомест, средствата би се распоредувале согласно важечките правила на ФИНКИ за апликативни проекти.
   Како иницијален чекор е дисеминирањето на информацијата за постоењето на оваа форма до сите вработени и сите студенти, како единствена точка на контакт каде треба да ги пријавуваат проблемите поврзани со компјутерската безбедност.
3. Развој на CSIRT план за проект.
   Планот за работа на CSIRT на ФИНКИ е даден во овој документ. Заради подобро функционирање, како и за јакнење на улогата на оваа организација, потребно е да се формира во вид на центар при Факултетот, како и да се назначи негов раководител.
   Одговорности на раководителот ќе бидат
   - Застапување на интересите на CSIRT пред управата на факултетот
   - Воспоставување контакти со сите други слични организации на државно и меѓународно ниво
   - Организација на работата на CSIRT
   - ….
4. Собирање на информации.
   Раководителот, во соработка со членовите на тимот треба да обезбеди вклучување на CSIRT на ФИНКИ во комуникациските канали и мрежите на вакви

организации на ниво на државата, но и на меѓународно ниво. Една од главните задачи на тимот ќе биде редовното објавување на релевантни информации на веб страницата на CSIRT (истата е во финална фаза на изработка)

5. Идентификување на CSIRT структура во организацијата.

   Во овој чекор се дефинира CSIRT на кого нуди услуги и поддршка. Во нашиот случај тоа се студентите и вработените при ФИНКИ.

6. Дефинирање на мисијата на CSIRT.

   Мисијата на креирање на CSIRT на ФИНКИ е да се обезбеди детектирањето, решавањето и превенцијата во врска со безбедноста на информациите и мрежата при факултетот.

7. Одлучување на опсегот и рангот на услугите CSIRT што ќе ги понуди.

   Во овој чекор ќе ги дефинираме примарните услугите кои CSIRT ќе ги нуди. Ќе опфатиме услуги од трите категории услуги кои CSIRT ги нуди:

   - Реактивни: справување со инциденти, справување со слабости
   - Проактивни: мониторирање на безбедноста на информациите, развивање на security tools
   - Безбедносни: анализа на ризици, едукација и тренинг,

8. Идентификување на потребните ресурси како вработени, опрема и инфраструктура за CSIRT.

   Тековната инфраструктура на ФИНКИ би се искористила како почетна инфраструктура на CSIRT. За почеток, потребно е подигање на веб страницата на CSIRT, воспоставување на соодветните мејлинг листи, креирање на контакт точките (пред се email адреса за пријавување на проблеми и веб базиран интерфејс).

9. Организациска структура

   Заради подобро функционирање на CSIRT, истиот треба да има едноставна структура која ќе дозволи поголема флексибилност и еластичност. Особено е битни да се назначат одговорни лица за трите главни типови на услуги кои ќе ги нуди: реактивни, проактивни и безбедносни. Поради ограничените ресурси, едно лице може да биде носител на повеќе улоги.

10. Дефинирање на интеракцијата и интерфејсот кон CSIRT.

    Идентификување на интеракцијата и интерфејсот за пријавување на инцидентот. Воспоставање на соодветна email адреса и веб сајт со понудена форма за пријавување на инцидент. На веб сајтот би имало објаснување на стандардни документи за испраќање на информацијата до организацијата. Сите овие пријави ќе се чуваат и ќе ја формираат базата на знаење на CSIRT. Дополнително, воведување на пракса за заведување на инцидентите кои се пријавени не преку овие два канали (лично, на телефон,...) заради збогатување на базата на знаење.

11. Дефинирање на улогите и одговорностите во CSIRT.

    Дефинирање на разни улоги во склоп на CSIRT. Потребно е да имаме улоги и интерфејси помеѓу различни CSIRT со што ќе се овозможи надворешна комуникација и соработка.

    Во овој дел, особено е битно да се работи на дефинирање на Стандардни оперативни процедури со кои би се решавале одредени типови на инциденти, а кои многу би помогнале во унифицираниот пристап кон решавањето. Списокот на процедури ќе биде дефиниран во посебен документ.

12. Објавување на CSIRT дека станува функционален.

Со испраќање на известување по сите официјални канали за комуникација (мејлин листи, форуми, courses и сл.) да се дистрибуира веста дека CSIRT станува функционален. Истото за да биде поефективно може да се дели рекламен материјал на кампусот, како и во онлајн верзија на социјалните мрежи.

13. Дефинирање методи за еволуирање на CSIRT.

Дефинирање на критериуми и параметри за квалитет така што при мерење на ефикасноста на CSIRT ќе се добијат релевантни информации. Дефинирање на методи за добивање повратни информации од организацијата.
Имплементирање на репорти кои ќе ја мерат ефикасноста на CSIRT.

Кои услуги ќе ги понуди CSIRT?

Бидејќи овој CSIRT ќе биде иницијален ќе се фокусираме услугите кои ќе ги нуди да бидат квалитетни, а бројот да биде соодветен. За таа цел ќе ги понудиме следните услуги со тоа што во иднина бројот на услуги ќе се зголемува:

- Поддршка за IT администраторите во кампусот во однос на прашања и информации поврзани со безбедноста
- Поддршка на студентите во решавањето на безбедносните проблеми
- Известување на други CSIRT, CERT доколку се идентификува директен напад
- Едукација на корисниците за безбедност
- Конфигурирање и одржување на безбедносни алатки, апликации и инфраструктура
- Справување и анализа на инциденти
- Истражувачки активности

Веб страна

Референци

https://www.terena.org/activities/tf-csirt/starter-kit.html

http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm

http://www.cert.org/incident-management/services.cfm

http://resources.sei.cmu.edu/asset_files/WhitePaper/2006_019_001_53104.pdf