Българска асоциация
за развитие на знанията
за информационните и
комуникационни технологии

МТФ
СИЛАТА НА ТЕХНОЛОГИИТЕ

КИБЕРСИГУРНОСТ, РИСКОВЕ И ЗАЩИТА НА ЛИЧНА ИНФОРМАЦИЯ И ДАННИ

к–н маг. юр.
МАРИЯ ДОЧЕВА
юрисконсулт в служба
“Военна полиция”
Докторант в ТУ-София

маг. инж.
ДИМИТЪР ДИМИТРОВ
Докторант в ТУ–София

СЪДЪРЖАНИЕ

ЧАСТ 1 – Потребителски профили

- Възстановяване на USB Flash – демонстрация
- Индустрия
- Задължения на ЮЛ и ФЛ
- Възможни защити

ЧАСТ 2 – Чувствителна информация

- Пример за откраднати данни за потребителски профили
- Юридически аспекти
- Новото в GDPR
- Възможни защити

ЧАСТ 3 – Лична кореспонденция

- Прихващане на кореспонденция
- Заплахи, Man In The Cloud - описание
- Мобилен телефон – пример
- ЗЕС
- Възможни защити

ЧАСТ 4 – Идентификационни данни

- Модифициране на карти за достъп
- Препоръки за ЮЛ
- Добри практики - ISO, NIST, BSI

ФИНАЛНА ДИСКУСИЯ

ПОТРЕБИТЕЛСКИ ПРОФИЛИ

Част 1

Пример за откраднати данни за потребителски профили

41 GB пароли,
Данни за 1.4 милиарда потребителски профила в явен вид…

Рекорд за компрометиране

Най-голямата кражба на данни за потребителски профили в историята

ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14

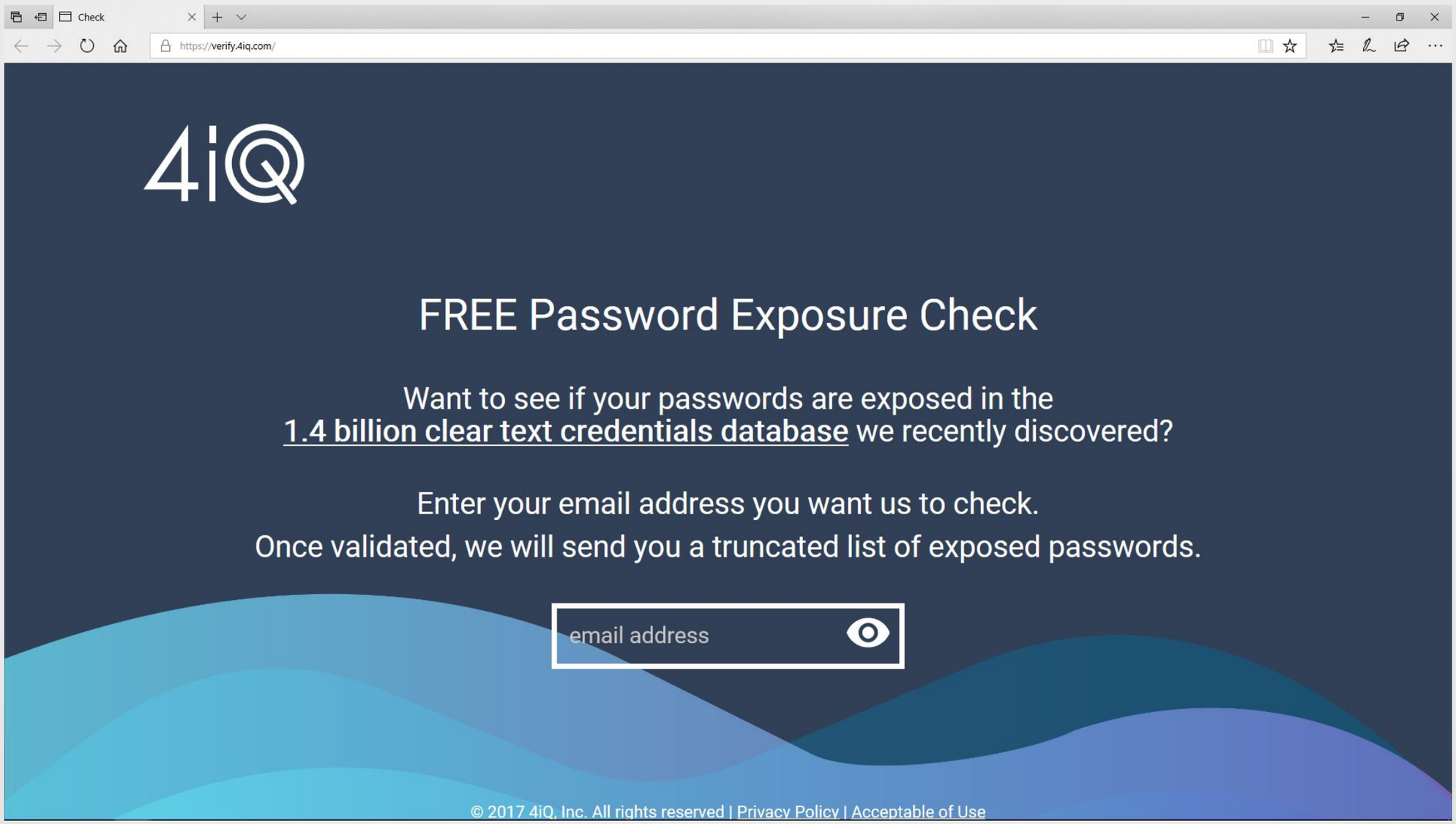
Просто статистика

На 05.12.2017 г. в Интернет се появява най-голямата до момента база данни с хакнати пароли -1,4 милиарда различни пароли с обем 41 GB.

	Count	Password
1	9218720	123456
2	3103503	123456789
3	1651385	qwerty
4	1313464	password
5	1273179	111111
6	1126222	12345678
7	1085144	abc123
8	969909	1234567

Аз там ли съм?

https://verify.4iq.com/



Възможни защити

Възможни защити (потребител)

- Обновяване на ОС, драйвери и приложения
- Антивирусни продукти
- Защитна стена (firewall)
- „Надеждна“ парола
- Смяна на парола
- Свеждане до необходимия минимум на разпространението на имената на акаунтите за електронна поща и др. услуги

Юридически аспекти

Юридически аспекти

- КОНВЕНЦИЯ № 108 на Съвета на Европа от 28.01.1981 г. за защита на лицата при автоматизираната обработка на лични данни

Лични данни (1)

- Целта на Конвенцията е да гарантира на територията на всяка страна за всяко физическо лице, независимо от неговата националност и местопребиваване, зачитане на неговите права и основни свободи и по-конкретно правото му на личен живот по отношение на автоматизираната обработка на лични данни, отнасящи се до него (“защита на данните”)
- Всяка страна по Конвенцията се задължава да предприеме необходимите мерки във вътрешното си право за влизане в сила на основните принципи за защита на личните данни
- Конвенцията унифицира правните разпоредби за защитата на правата на гражданите на страните - членки на Съвета на Европа, по отношение на автоматизираната обработка на лични данни за тях

Лични данни

- В изпълнение на Конвенцията страните се задължават да я прилагат спрямо автоматизираните регистри с лични данни и автоматизираната обработка на лични данни в обществения и частния сектор
- Предвидена е възможност във всеки момент всяка държава да уведоми чрез декларация до главния секретар на Съвета на Европа, че разширява обсега на действие на Конвенцията по отношение на регистри с лични данни, които не са обект на автоматизирана обработка, или че изключва определени категории регистри с лични данни

Лични данни

- Всяка страна се задължава да установи съответни санкции и да предвиди възможност за обжалване при нарушаване на разпоредбите на вътрешното си право, в което са залегнали принципите за защита на данните, посочени в Конвенцията.
- **Конвенцията не допуска изразяване на резерви по нейните разпоредби.**
- В съответствие с последователно изразяваните препоръки на Европейската комисия, Народното събрание прие Закон за защита на личните данни, в сила от 1 януари 2002 г., с което Република България изпълни задължението си по чл. 4 от Конвенцията.

Лични данни

Според Закона за защита на личните данни (ЗЗЛД):

- „Лични данни“ са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.
- „Обработване на лични данни“ е всяко действие или съвкупност от действия, които могат да се извършат по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.

Цел и приложение на ЗЗЛД

- Гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните.

- Прилага се, когато администраторът на лични данни:
  - е установен на територията на Р България и обработва лични данни във връзка със своята дейност;
  - не е установен на територията на Р България, но е задължен да прилага ЗЗЛД по силата на международното публично право;
  - не е установен на територията на държава-членка на ЕС, както и в друга държава-членка на ЕИП, на за целите на обработването използва средства, разположени на българска територия, освен когато тези средства се използват само за транзитни цели

Цел и приложение на ЗЗЛД

- Прилага се при обработване на лични данни за целите на:
  - отбраната на страната
  - националната сигурност
  - опазване на обществения ред и противодействието на престъпността
  - наказателното производство
  - изпълнението на наказанията
- Не се прилага за обработване на лични данни, извършвано от физически лица за техни лични или домашни дейности, както и за информацията, която се съхранява в Националния архивен фонд

Закон за защита на личните данни

- Обработването на лични данни е допустимо, когато е налице поне едно от следните условия:
  - обработването е необходимо за изпълнение на нормативно установено задължение на администратора на лични данни
  - физическото лице, за което се отнасят данните, е дало изрично своето съгласие
  - обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и за действия, предхождащи сключването на договор и предприето по негово искане

Закон за защита на личните данни

- обработването е необходимо, за да се защитят животът и здравето на физическото лице, за което се отнасят данните
- обработването е необходимо за изпълнение на задача, която се осъществява в обществен интерес
- обработването е необходимо за упражняване на правомощия, предоставени със закон на администратора или на трето лице, на което се разкриват данните
- обработването е необходимо за реализиране на законните интереси на администратора на лични данни или на трето лице, на което се разкриват данните, освен когато пред тези интереси преимущество имат интересите на физическото лице, за което се отнасят данните

Закон за защита на личните данни

- Обработването на лични данни е забранено, когато:
  - разкриват расов или етнически произход
  - разкриват политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели
  - се отнасят до здравето, сексуалния живот или до човешкия геном

освен когато:

Закон за защита на личните данни

- Обработването е необходимо за целите на изпълнението на специфични права и задължения на администратора в областта на трудовото законодателство
- Физическото лице, за което се отнасят тези данни, е дало изрично своето съгласие за обработването им, освен ако в специален закон е предвидено друго
- Обработването е необходимо за защита на живота и здравето на физическото лице, за което тези данни се отнасят, или на друго лице и състоянието на физическото лице не му позволява да даде съгласие или съществуват законни пречки за това

Закон за защита на личните данни

- Обработването се извършва от организация с нестопанска цел, включително с политическа, философска, религиозна или синдикална цел, в хода на законосъобразната ѝ дейност и с подходяща защита, при условие че:
  - обработването е свързано единствено с членовете на тази организация или с лица, които поддържат редовни контакти с нея във връзка с нейните цели
  - данните не се разкриват на трети лица без съгласието на физическото лице, за което те се отнасят

Закон за защита на личните данни

- Обработването се отнася до данни, публично оповестени от физическото лице, или то е необходимо за установяването, упражняването или защитата на права по съдебен ред
- Обработването е необходимо за целите на превантивната медицина, медицинската диагностика, предоставянето или управлението на здравни услуги, при условие че данните се обработват от медицински специалист, задължен по закон да пази професионална тайна, или от друго лице, обвързано с подобно задължение за опазване на тайна
- Обработването се извършва единствено за целите на журналистическата дейност, литературното или художественото изразяване, доколкото то не нарушава правото на личен живот на лицето, за което се отнасят тези данни

Закон за защита на личните данни

- По силата на Закона за защита на личните данни е създадена Комисия за защита на личните данни (КЗЛД) като независим държавен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Закона за защита на личните данни
- Членовете на комисията и председателят й се избират от Народното събрание по предложение на Министерския съвет

Производства пред КЗЛД

- разглеждане на жалби
- регистрация на администратори на лични данни
- издаване на разрешения
- изразяване на становища
- издаване на задължителни предписания
- налагане на временни забрани за обработване на лични данни
- заличаване на администратори на лични данни
- Комисията може да осъществява и други производства, когато това е предвидено в закон

Други регламентиращи документи

- РЕГЛАМЕНТ (ЕО) № 45/2001 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 18 декември 2000 година относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни
- ДИРЕКТИВА 95/46/ЕО НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (отм. с Регламент № 2016/679)

Новото в GDPR

Новото в GDPR

На 27 април 2016 г. бе приет нов регламент в областта на личните данни, а именно Регламент 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО. Регламентът вече е в сила, но ефективно ще се прилага от 25 май 2018 г.

Новото в GDPR

- Във връзка с развитието на научните и техническите ресурси е разширен обхватът на видовете признаци, по които едно лице може да бъде идентифицирано пряко или непряко и които се включват в понятието "лични данни":
  - име
  - идентификационен номер
  - данни за местонахождение
  - онлайн идентификатор

  или по един или повече признаци, специфични за физическата, физиологичната, **генетичната**, психическата, умствената, икономическата, културната или социалната идентичност на това физическо лице.

Новото в GDPR

- Легална дефиниция на:
  - "генетични данни" - лични данни, свързани с наследствени или придобити генетични белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице
  - "биометрични данни" - лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни
  - "данни за здравословното състояние" - лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние

Новото в GDPR

- Пояснено е, че обработването на снимки не следва систематично да се счита за обработване на специални категории лични данни, тъй като снимките се обхващат от определението за биометрични данни единствено когато се обработват чрез специални технически средства, позволяващи уникална идентификация или удостоверяване на автентичността на дадено физическо лице
- не се изисква географска свързаност на администратора на лични данни с Европа
- предвижда се наличие на съгласие на субекта на лични данни за обработването им за една или повече конкретни цели като едно от алтернативно изброените условия за законосъобразност

Новото в GDPR

- Поставят се завишени изисквания към съгласието - то трябва да е изрично и недвусмислено (мълчанието, предварително отметнатите полета или липсата на действие не представляват съгласие)
- Изпълнението на даден договор или предоставянето на услугата не се поставя в зависимост от даване на съгласие за обработване на лични данни във всички случаи, когато такива данни не са необходими за изпълнението на договора или за предоставяне на услугата
- Специални правила относно съгласието, давано за обработката на лични данни на деца

Новото в GDPR

- Права на субектите на лични данни:
  - право "да бъдеш забравен" - изтриване на данни по искане на субекта при наличие на предвидените в Регламента предпоставки. Администраторът е длъжен без ненужно забавяне да изтрие данните на лицето
  - право на ограничаване на обработването, право на коригиране и допълване
  - право на информация и достъп
  - право на възражение - при отправено възражение администраторът е длъжен да преустанови обработването на данните, освен ако не докаже, че съществуват убедителни законови основания за обработването

Новото в GDPR

- право на защита - ако субектът на лични данни счита, че обработването на данните, отнасящи се до него, е в противоречие на Регламента, той има право да подаде жалба до надзорен орган (КЗЛД). Освен това субектът има право да защитава нарушените си права и по съдебен ред пред съдилищата на държавата, в която е установен нарушителят. Освен тези две възможности, субектът на лични данни има право и на ефективна съдебна защита срещу надзорния орган. Предоставена е и възможност за предявяване на искове за обезщетение за причинени от администраторите или обработващите лични данни материални и нематериални вреди;
- право на преносимост на данните;

Новото в GDPR

- засилена отговорност на администраторите на лични данни - според разпоредбите на Регламента, отговорността при нарушение на правилата закопаване на лични данни е при всяко лице, което има досег до тях (администраторите и обработващите лични данни). Администраторът е длъжен да вземе такива подходящи мерки, чрез които да може да докаже, че данните се обработват в съответствие с изискванията на Регламента. Въвежда се изискването за защита на данните на всяко ниво - както към момента на определяне на средствата за обработване, така и към самото обработване. Към техническите мерки може да бъде използвана псевдонимизация

Новото в GDPR

- Администраторите и обработващите лични данни са длъжни да водят регистри на дейностите по обработване;
- Въвеждане на принципа "свеждане на данните до минимум";
- Създава се нов общоевропейски надзорен орган - Европейски комитет по защита на данните;
- Завишени санкции за нарушение на изискванията за сигурността на данните:
  - при нарушаване на изискванията за съгласие при събиране и обработване на данните, когато такива се изисква, неспазване на разпореждане на надзорен орган и др., глобата или имуществената санкция може да достигне до 20 млн. евро или до 4 % от годишния световен оборот на предприятието за предходната финансова година. За някои други нарушения санкцията достига до 10 млн. евро или до 2 % от годишния световен оборот на предприятието за предходната финансова година

Новото в GDPR

- На всяка държава-членка е предоставена възможността да определя дали и до каква степен могат да бъдат налагани административни наказания глоба или имуществена санкция спрямо собствените й публични органи и структури
- Длъжностно лице по защита на данните (ДЛЗД):
  - ролята на ДЛЗД е да оказва съдействие за спазването на разпоредбите на Регламента
  - не носи лична отговорност при неспазване на Регламента
  - ДЛЗД се определя въз основа на неговите професионални качества и по-специално въз основа на експертните му познания в областта на законодателството и практиките в областта на защитата на данните
  - ДЛЗД може да бъде членна персонала на администратора или обработващя лични данни, или да изпълнява задачите въз основа на договор за услуги, сключен с физическо лице или организация, извън организацията на администратора

Новото в GDPR

- Отпада задължението на администраторите на лични данни да се регистрират в Комисията за защита на личните данни;
- Принцип "обслужване на едно гише" при трансгранична обработка на данни

Възможни защити (доставчик)

- Надеждна автентикационна схема
- Локализация на активността по географски принцип
- Многостъпкова автентикация с използването на повече от едно устройство
- Еднократни пароли

ЧУВСТВИТЕЛНА ИНФОРМАЦИЯ

Част 2

Възстановяване на ДАННИ от USB флаш памет

Демонстрация

Демонстрация

Демонстрация

Демонстрация

Възможни защити

Възможни защити

- Криптиране
- Мерки за физическа защита при напускане на охраняемата зона или зоната за сигурност на организацията (респ. на дома) с цел мономизиране на вероятността от кражба или загуба на носителя
- Физическо изтриване на информацията (за flash-базиран носител на информация този вид изтриване не е надежден)
- Създаване на организация за събиране (депониране) на повредена или излязла от употреба електроника, която съдържа носители на информация

Индустрията

Задължения на юридическите и физическите лица

Юридическо лице - администратор на лични данни

- Определяне на ред и отговорни служители за транспонирането на нормите на Регламента в дейността на юридическото лице
- Определяне на длъжностно лице за защита на данните
- Определяне на техническите и организационни мерки, които ще се прилагат
- Информиране на служителите при наличие на видеонаблюдение
- Изготвяне и приемане на вътрешни правила за:
  - защита на личните данни;
  - действие при нарушаване на сигурността на личните данни;
- Водене на регистър на дейностите по обработването на личните данни.

Физическо лице - обработващ лични данни

- Предоставяне на достатъчно гаранции за прилагането на подходящи технически и организационни мерки
- Обработва личните данни само по документирано нареждане на администратора
- Гарантира че лицата оправомощени да обработват личните данни са поели ангажимент за поверителност или са задължени по закон да спазват поверителност
- Взема всички необходими мерки за осигуряване сигурността на обработването на личните данни
- Подпомага администратора на лични данни

Класифицирана информация

- Закон за защита на класифицираната информация;
- Правилник за прилагане на закона за защита на класифицираната информация.
  - служебна тайна;
  - държавна тайна.
- Приемане на вътрешни правила, регламентиращи реда за изготвяне и съхранение на документи, съдържащи класифицирана информация, както и отговорността на служителите, обработващи такава информация.

ПОЧИВКА

15 Минути

ЛИЧНА КОРЕСПОНДЕНЦИЯ

Част 3

Прихващане на електронна кореспонденция

Заплахи

Заплахи

- Фишинг
- Men In The Middle
- Men In The Cloud
- Други

Man In The Cloud

Пример

Същност

- Използва услугите за синхронизация на файлове
- GoogleDrive, OneDrive, Dropbox и др.
- Инфраструктурата за Command&Control (C&C)
- Извличане на данни
- Отдалечен достъп
- Без използване на exploit инструменти
- Трудно се установява от общите мерки за сигурност в системата

Обективни констатации

- Услугите за синхронизиране на файлове могат лесно да се превърнат в инфраструктура за компрометиране на крайните точки, предоставяйки канал за C&C, извличане на данни и отдалечен достъп
- Услугите могат да бъдат компрометирани без да се налага използването на идентификационни данни в явен вид
- Възстановяване на компрометираните профили за синхронизиране на файлове не винаги е възможно (т.е. профилът трябва да бъде затворен)
- Атаките, базирани на горепосочената архитектура, не са нови (напр. "The Inception Framework", анализирана от Blue Coat Labs)
- Не съществува злонамерен код за крайната точка и не се наблюдават необичайни изходящи канали за трафик
- Мониторинг и защита на данните както в облака, така и на място
- Идентифицирането на модели за злоупотреба с такава архитектура от ново поколение е в основата на защитата.

Факти (1)

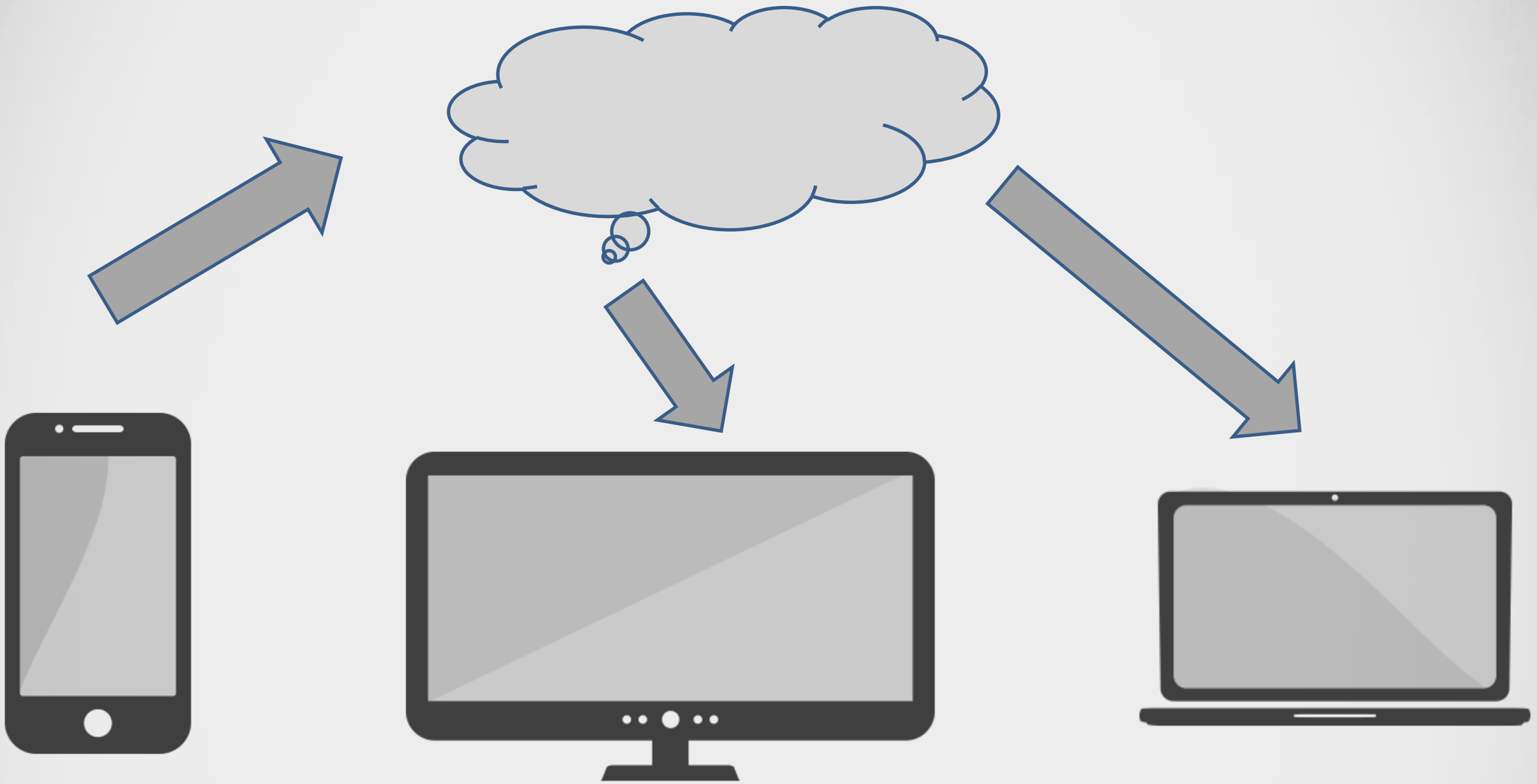
- През последните няколко години станахме свидетели на масови пробиви на сигурността и нарушения на данни
- Големи компании бяха притеснени от хакери, загубите са за милиарди долари, мениджъри загубиха работата си
- Кредитни карти, личната идентификационна информация и интелектуалната собственост се крадат ежедневно и се търгуват в тъмната страна на мрежата срещу Bitcoins
- С увеличаването на атаките, "атакуваната повърхност", достъпна за нападателите, също нараства
- И частните лица, и всички бизнес институции, преминават от локални приложения към облачни услуги

Факти (2)

- Услугите за синхронизиране на файлове правят данните достъпни за множество потребители и устройства - понякога в различни държави и организации
- С увеличената употреба на мобилни устройства, таблети, VPN, отдалечен работен плот и приложения от типа SaaS (Software as a Service), все повече данни се съхраняват в облака, където потенциално се разпространяват извън определени физически граници
- Границите на съхранението на данни стават все по-малко дефинирани, следователно все по трудно се определят мерките за защита на периметъра
- Когато няма ясен периметър, който да се защити, е много трудно лицето или организацията да се предпазят от изтичане на данни или от зловреден софтуер

Услуги за синхронизиране

- GoogleDrive, Dropbox, OneDrive, Box и др. – синхронизиране на файлове
- Позволяват на дадено лице (потенциално служител на предприятие) да съхранява синхронизирани копия на хранилища на файлове на множество устройства
- Свързване на устройствата, използвани от дадено лице, с централен хъб в облака, идентифицирайки се с един и същ профил
- Всяка промяна в хранилището на файлове на едно устройство бързо се синхронизира с хъба и след това се разпространява на другите устройства
- Услугите за синхронизиране на файлове обикновено са конфигурирани да синхронизират съдържанието на конкретна локална папка с корпоративни машини в облака. Файловете, които са добавени локално към тази папка или са актуализирани, се качват в облака и файловете, заредени в облака, се изтеглят в конкретната локална папка



MOBILE

DESKTOP

PORTABLE

Механизъм на синхронизация

- Синхронизацията се осъществява чрез специализиран софтуер, инсталиран на крайната станция
- Софтуерът се предоставя от доставчика на услуги и се грижи за мониторинга на локалната папка за синхронизиране, както и на облачния център за евентуални промени
- Комуникацията с облачния център от името на потребителя изисква удостоверяване
- Повечето от услугите избягват използването на име на акаунта и парола, а удостоверяването става с помощта на синхронизиращ токен
- Предполагаемото предимство на токена пред метода със съхранение на парола е, че компрометирането на токена не компрометира целия профил. В резултат на това законният собственик на профила може да използва името и паролата, за да възстанови правата си върху профила и да отмени правата върху компрометирания токен

OAuth 2.0

- https://oauth.net by Aaron Parecki

- OAuth 2.0 Framework - RFC 6749
- В по-голямата си част анализираните услуги за синхронизация използват стандартния токен OAuth 2.0
- OAuth е предназначен за удостоверяване и оторизация между приложенията (Application Layer)
- Всяко копие на приложението, инсталирано в крайна станция, се разглежда като "приложение", а не като крайна станция. Т.е. на базата на токен OAuth 2.0 се изграждат отделни протоколни сесии за автентификация
- Това наблюдение обяснява някои от слабостите в сигурността, които посочваме по-късно

Мотивация

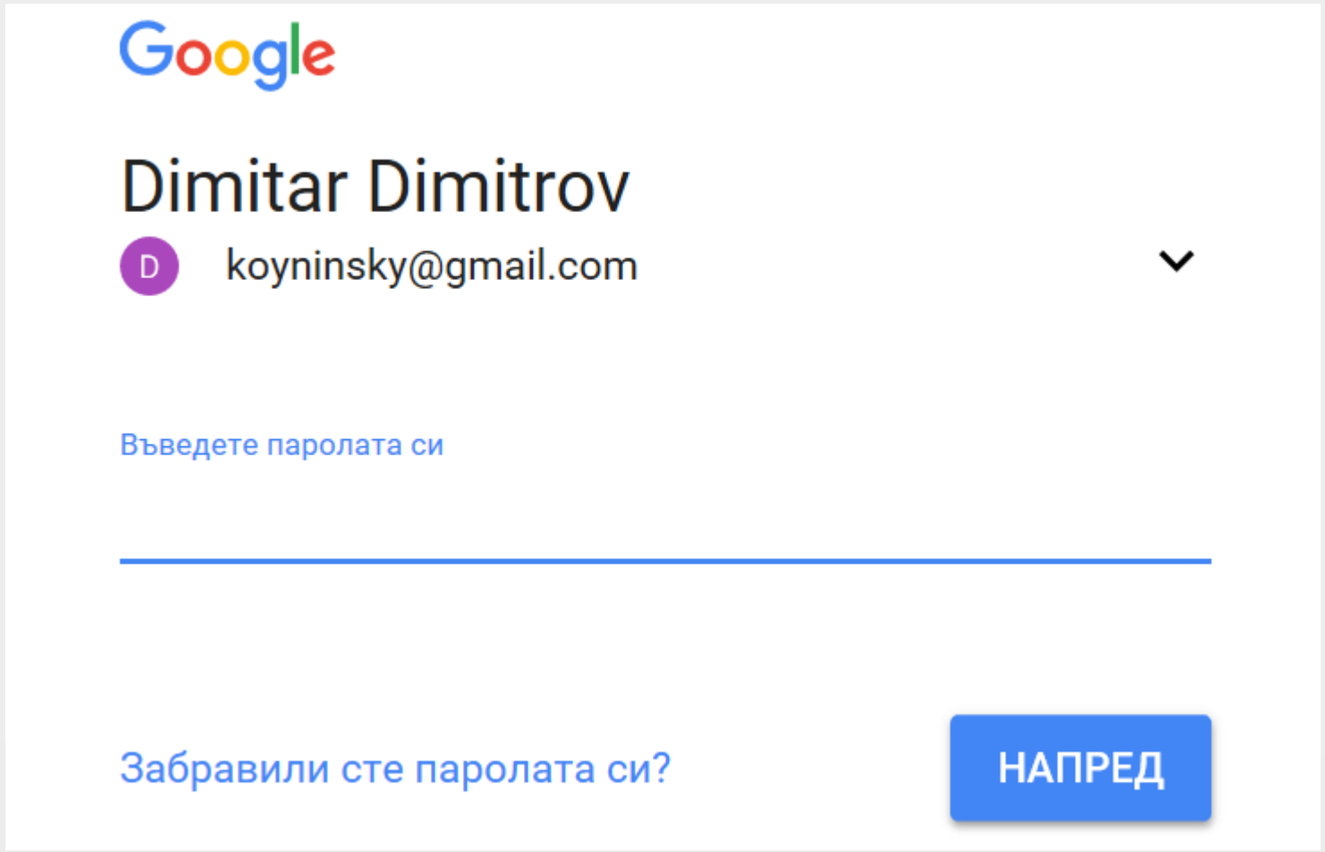
- Организациите отдават голямо значение на сигурността на крайните потребители и устройства
- По-старите решения често се основават на сравнение на шаблони с файлове, които може да съдържат злонамерен код
- По-новите решения се опитват да изпълняват входящи файлове в контролирана среда, за да разберат дали показват злонамерено поведение или да наблюдават активността на крайнитя потренител или устройство за такова злонамерено поведение. Това включва търсене на необичайни практики за инжектиране на код, възползване от известни уязвимости и други аномалии
- Някои решения се опитват да идентифицират C&C комуникацията чрез репутация или ранг (напр. черни списъци на IP адреси на известни C&C сървъри) или откриване на аномалии (напр. откриване на необичаен нов адрес, с който крайният потребител или устройство редовно комуникира)

Идеята

- Вместо да се опитваме да влезем в акаунта за синхронизиране на файлове на жертвата, установяваме, че е възможно синхронизирането на крайната точка на жертвата с акаунт, контролиран от нападател

Контролиране на целта (1)

- В хода на нормални операции, когато даден потребител на приложение за синхронизация иска да направи първоначална връзка с профил или да превключи между профили, от този потребител се изисква да предостави идентификационни данни за профила (име и парола) по интерактивен начин чрез графичен потребителски интерфейс

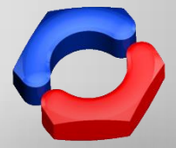


Контролиране на целта (2)

- Приложението за синхронизиране (в случая Google Drive) се основава на синхронизиращ токен, получен след горния процес на удостоверяване
- Токенът се използва за допълнителни операции след същинския процес на удостоверяване
- Той се съхранява в крайната точка или в регистъра, или във файл
- С други думи, след първоначалното удостоверяване не са необходими (или съхранявани) ясни идентификационни данни от дадено приложение, за да имат достъп до профила на потребителя
- Освен това лесно се установява, че синхронизиращият токен е независим от машината

Контролиране на целта (3)

- За всяко едно от приложенията за синхронизация просто копираме токена за профила на точното място в крайната станция и правим превключване на приложението за синхронизация към профила, представен от токена
- Следователно, нападателят може да получи достъп до профила на жертвата, като открадне токена и не е необходимо да компрометира или да придобива паролата на жертвата
- Не е нужно да използваме изрични идентификационни данни (обикновено име и парола за профила), което позволява атаката да не бъде открита от собственика на профила



Контролиране на целта (4)

- Таблицата показва обобщение на вида на токените и техните местоположения за съответното приложение

SYNCHRONIZATION APPLICATION	ONEDRIVE	BOX	GOOGLE DRIVE	DROPBOX
Token Type	OAuth Refresh Token	OAuth Refresh Token	OAuth Refresh Token	Proprietary
Location	Windows Credential Manager	Windows Credential Manager	Encrypted in Registry	Encrypted SQLite file

Контролиране на целта (5)

- Въз основа на констатациите, посочени в таблицата, е създаден инструмент, наречен "Switcher" за всяко от приложенията за синхронизация
- Инструментът взема като вход синхронизиращ токен и го съхранява на подходящото място на крайната станция на жертвата, за да се синхронизира с профила, представен от токена
- Токенът, подаван на Switcher, се извлича от машината на нападателя и представя акаунт, създаден (и контролиран) от нападателя
- Преди да направи превключването между профилите, Switcher запазва оригиналното означение от машината на жертвата във файл
- Този файл се копира от Switcher в папката за синхронизация непосредствено след превключването, така че оригиналният токен да бъде синхронизиран с акаунта, управляван от атакуващия

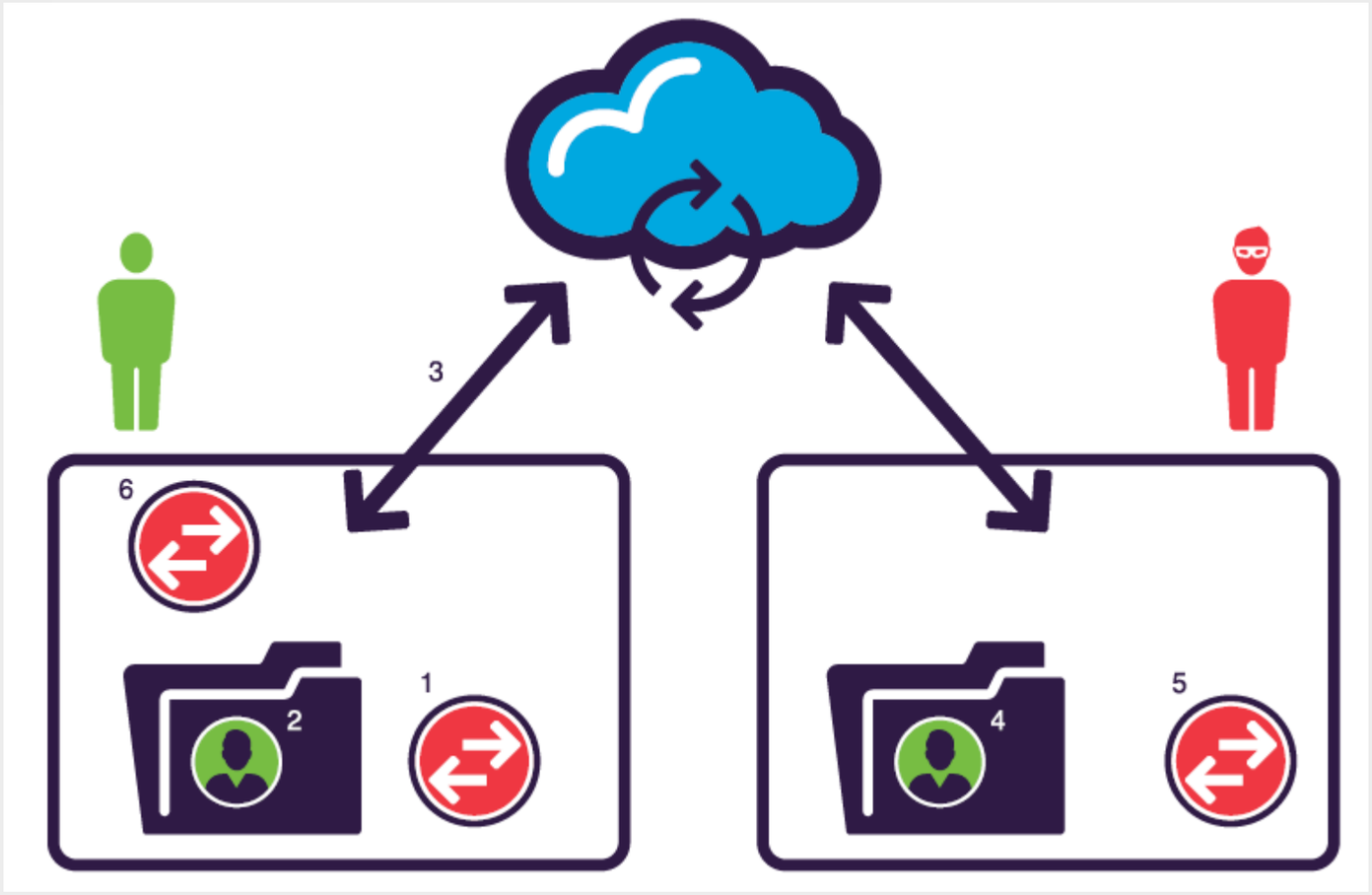
Контролиране на целта (6)

- Кодът на превключвателя Switcher е много прост
- Не взаимодейства с Интернет
- Не разчита на използването на вече известни уязвимости
- Модифицира някои специфични файлове или ключове в системния регистър
- Не засяга легитимен софтуер, поради което изключително трудно може да се определи като злонамерен код
- След като кодът на Switcher се изпълни, той може да бъде премахнат от крайната точка, без да остава никаква следа като доказателство за компрометирането

Бърз двоен превключвател (1)

- Тази доста проста атака позволява на атакуващия да споделя профила за синхронизиране на файлове на жертвата
- След това нападателят има достъп до файлове, синхронизирани от пострадалия, и заразява тези файлове със злонамерен код
- Нападението се състои в това, че се използва инструментът Switcher, споменат по-горе, на машината на жертвата
- Това може да се постигне чрез използване на drive-by-download уязвимост или чрез проста фишинг атака

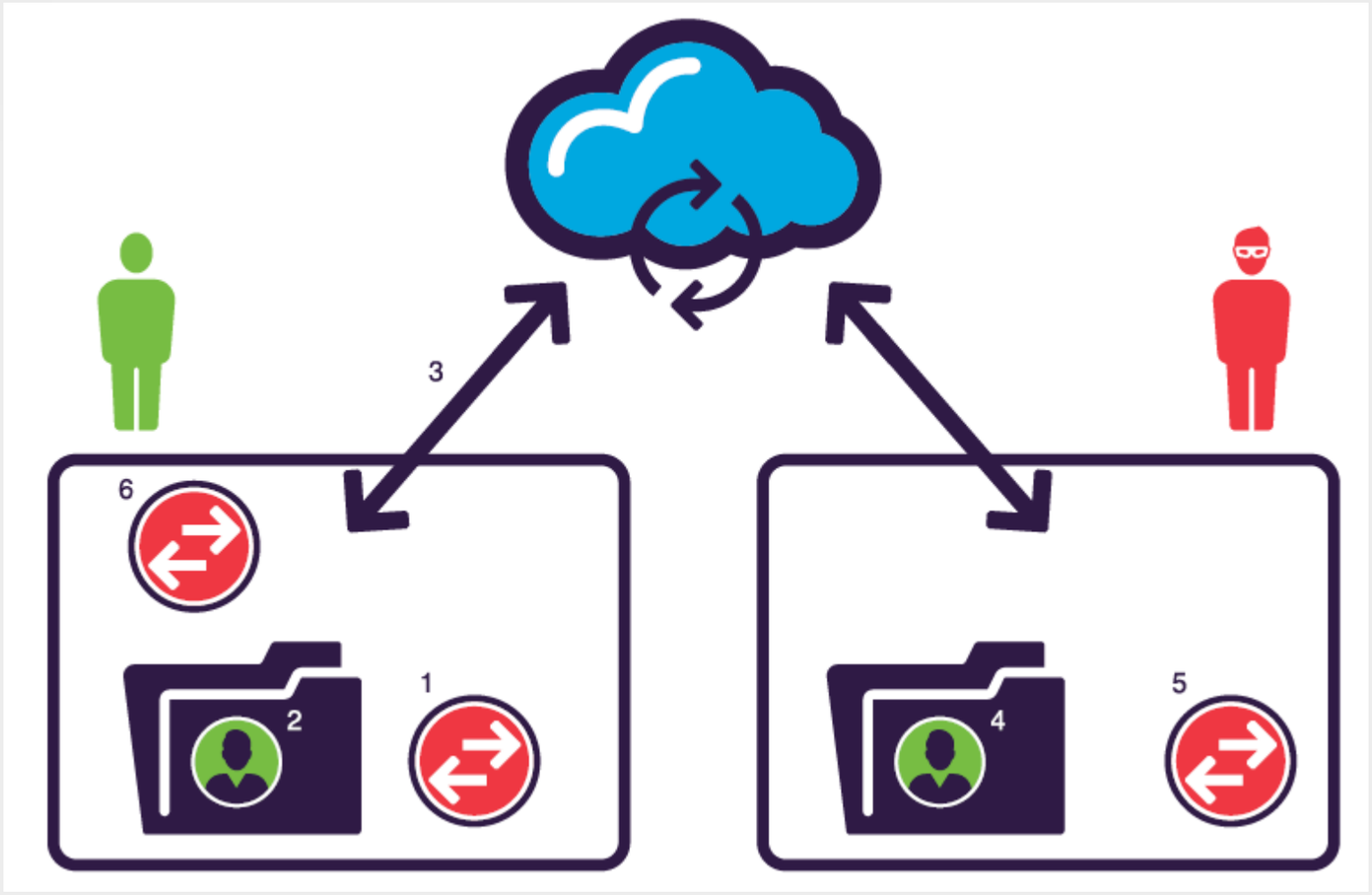
Последователност (1)



1. Нападателят подвежда жертвата (например чрез социално инженерство) или използва exploit, за да изпълни Switcher. След това Switcher инсталира синхронизационния токен на атакуващия в правилното място на приложението за синхронизация

ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf

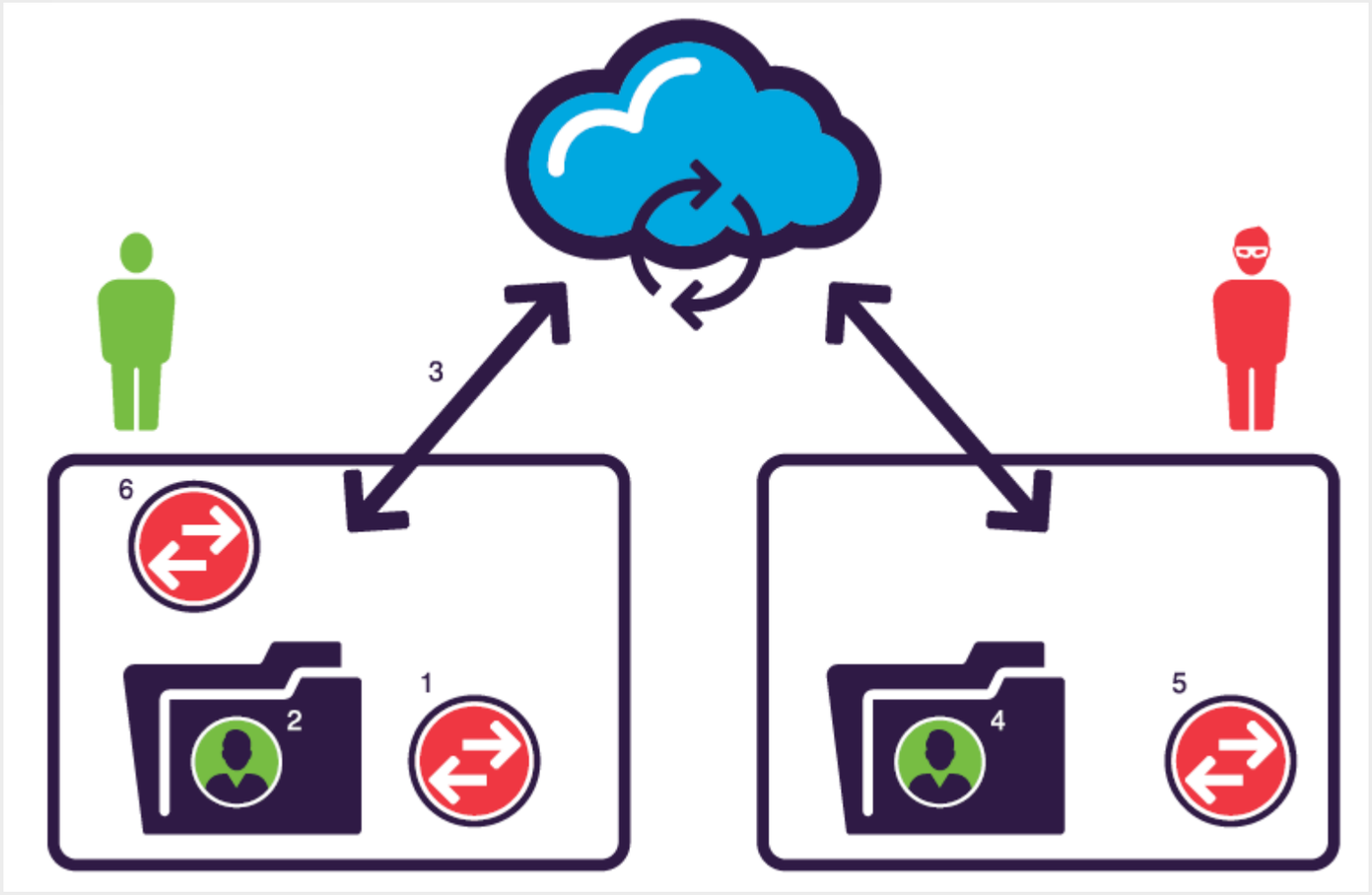
Последователност (2)



2. Когато първото превключване завърши, Switcher копира оригиналния синхронизационен токен в папката за синхронизация

ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf

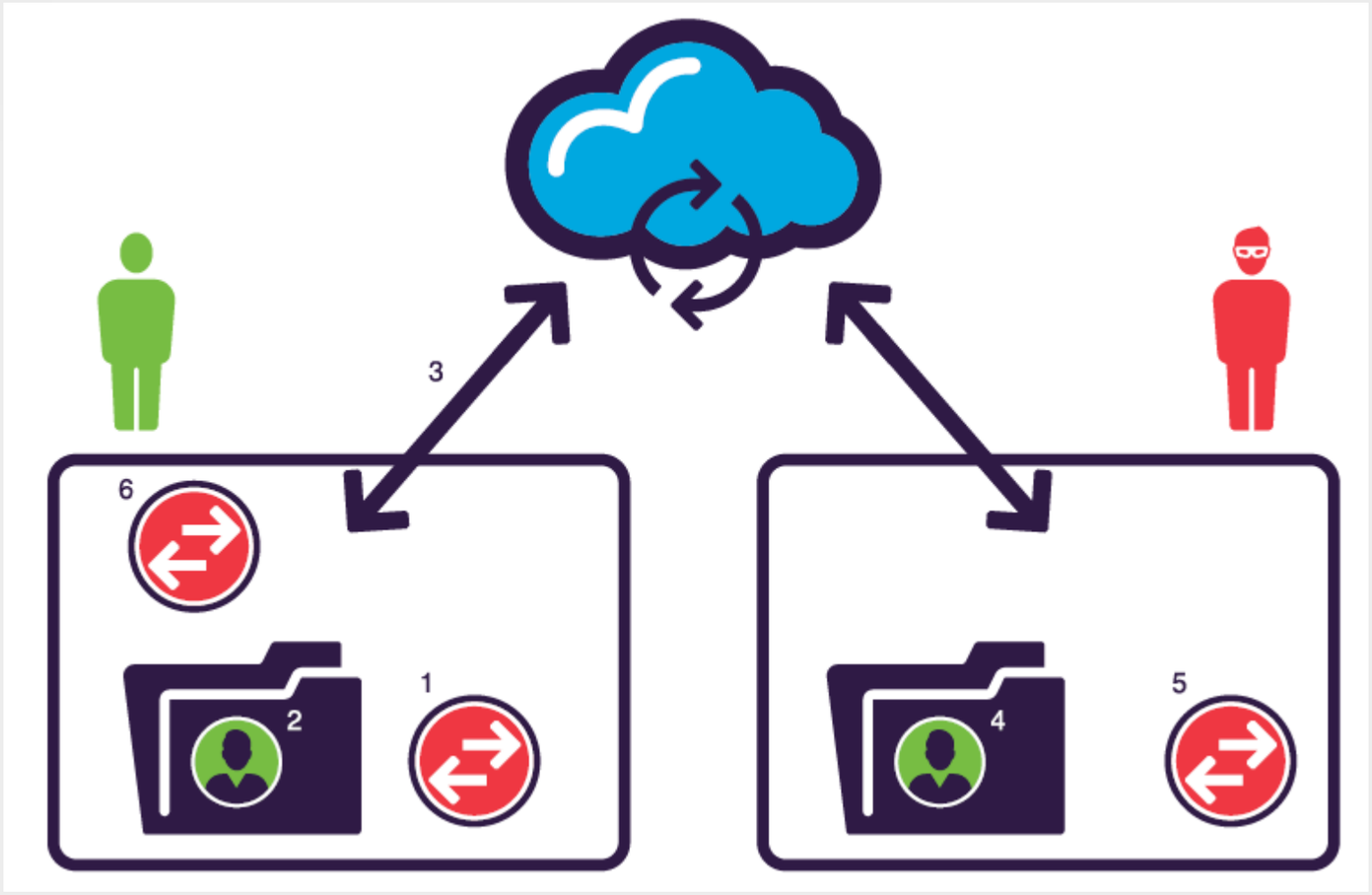
Последователност (3)



3. Drive приложението синхронизира съдържанието на синхронизационната папка с акаунта на атакуващия (в момента се използва автентикацинния токен на атакуващия)

ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf

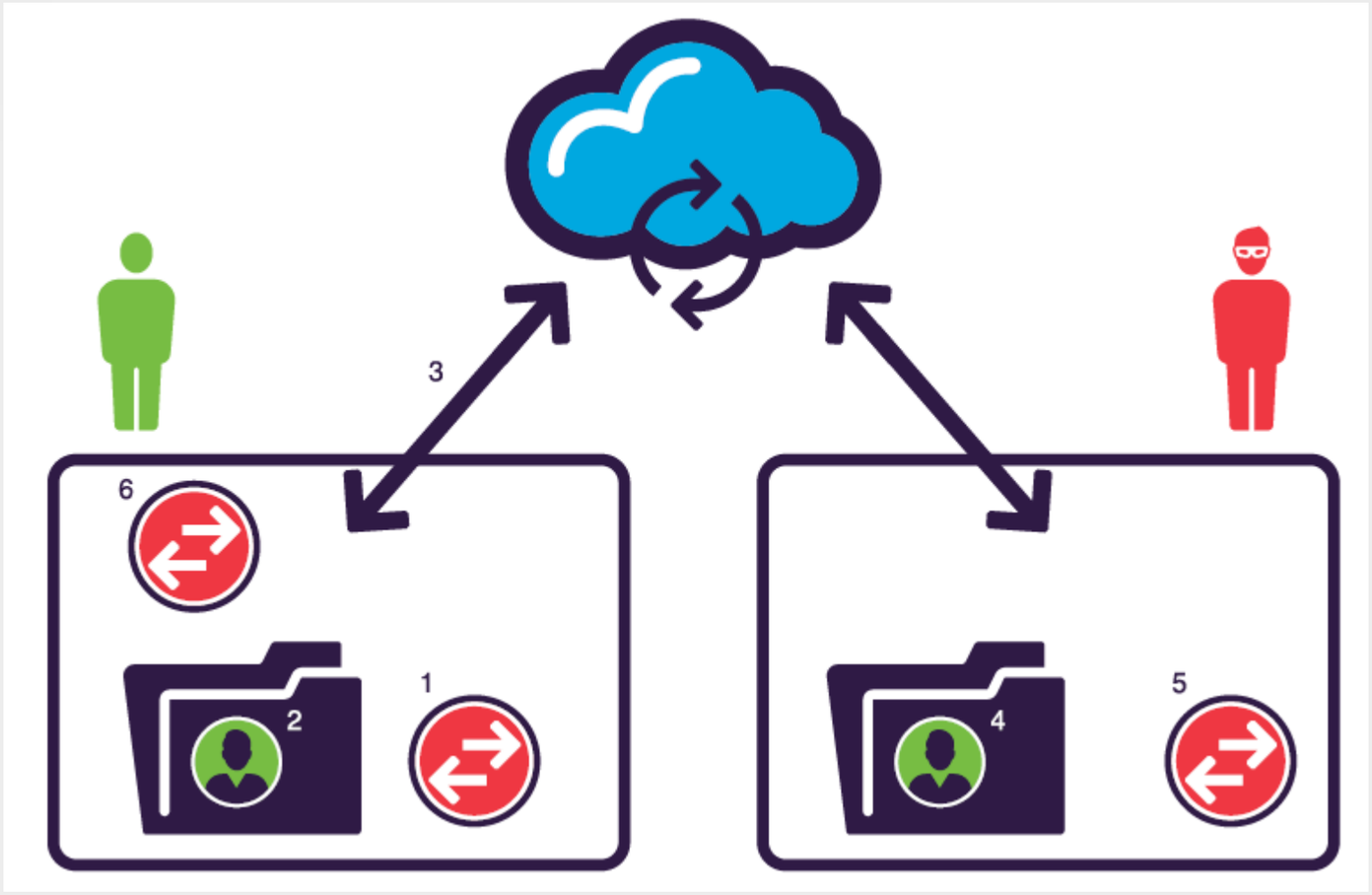
Последователност (4)



4. Така нападателят придобива токена за синхронизация на жертвата

ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf

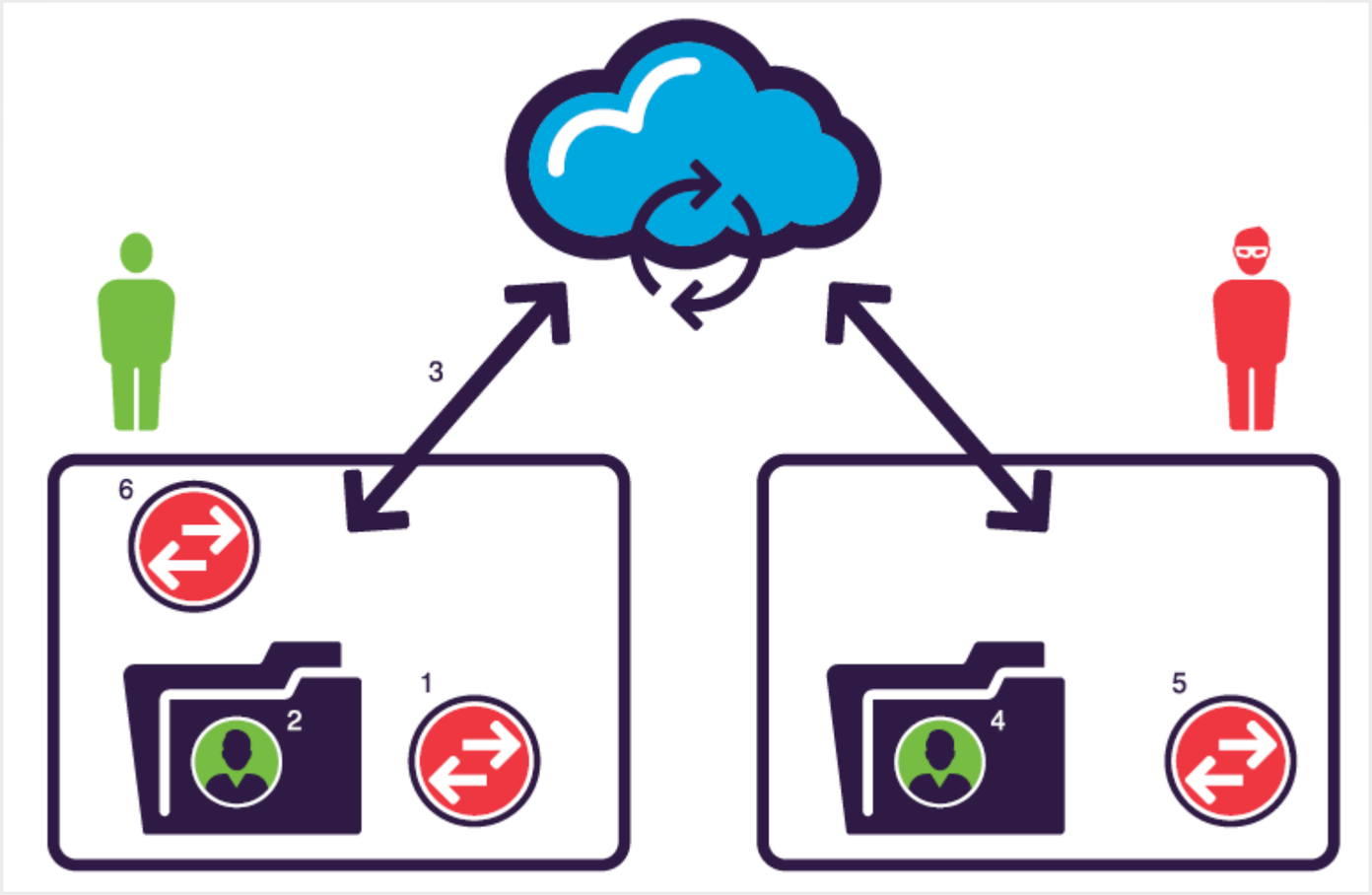
Последователност (5)



5. Атакуващият използва откраднатия синхронизиращ токен, за да се свърже с акаунта за синхронизиране на файлове на жертвата (например използвайки Switcher инструмента за превключване на машината на нападателя

ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf

Последователност (6)



6. Инструментът Switcher сработва за втори път на машината на пострадалия ("двоен ключ"), възстановявайки оригиналния токен за синхронизация на жертвата, като по същество възстановява приложението за синхронизация в първоначалното му състояние

ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf

Последствия (1)

- След като тази атака завърши, състоянието на приложението за файлово синхронизиране на жертвата е същото като преди атаката
- Кодът на Switcher се изтрива, което обикновено не оставя следи от злонамерен код
- След като атаката бъде завършена, данните, поставени от жертвата в папката за синхронизиране се синхронизират и с машината на нападателя

Последствия (2)

- Атаката с двоен превключвател може да бъде ефективна във времето, тъй като различните услуги за синхронизиране на файлове може да не ограничават достъпа до масивите от данни от няколко местоположения към профила за синхронизиране
- Докато Google реагира на необичаен достъп до самия Google профил (напр.: при свързването от ново устройство или от необичайно географско местоположение се изпраща e-mail съобщение към електронната поща на собственика), той не осигурява подобни сигнали за необичайна синхронизация. Следователно, е възможно за атакуващия да поддържа синхронизираща дейност с профила на жертвата отвсякъде, по всяко време и без уведомяване на собственика на профила

Последствия (3)

- В допълнение към прихващането на поверителна или лична информация, атакуващият може да манипулира файлове в папката за синхронизиране на машината на нападателя и промените да се разпространяват в машината на жертвата
- Например, атакуващият може да вмъкне Macro-код в MS Word документи или скриптове в PDF документи и да ги изпълнява, когато жертвата се опитва да получи достъп до тези файлове. Резултатите от изпълнението могат да бъдат записани в синхронизиращата папка и след това да се синхронизират с папката на нападателя
- След събирането на резултатите нападателят може да ги премахне от папката за синхронизиране и дори да възстанови оригиналния манипулиран документ, за да премахне всички следи от атаката

Последствия (4)

- Възможно е да се разработят и други потенциални атаки въз основа на бързия двоен ключ
- Една от възможностите е форма на Ransomware, в която атакуващият криптира файловете на жертвата
- Атакуващият ги синхронизира с всички други устройства, които се синхронизират и с профила на жертвата
- Тъй като атакуващият разполага с ключа за декриптиране, може да демонстрира пред жертвата, че е в състояние да възстанови информацията му

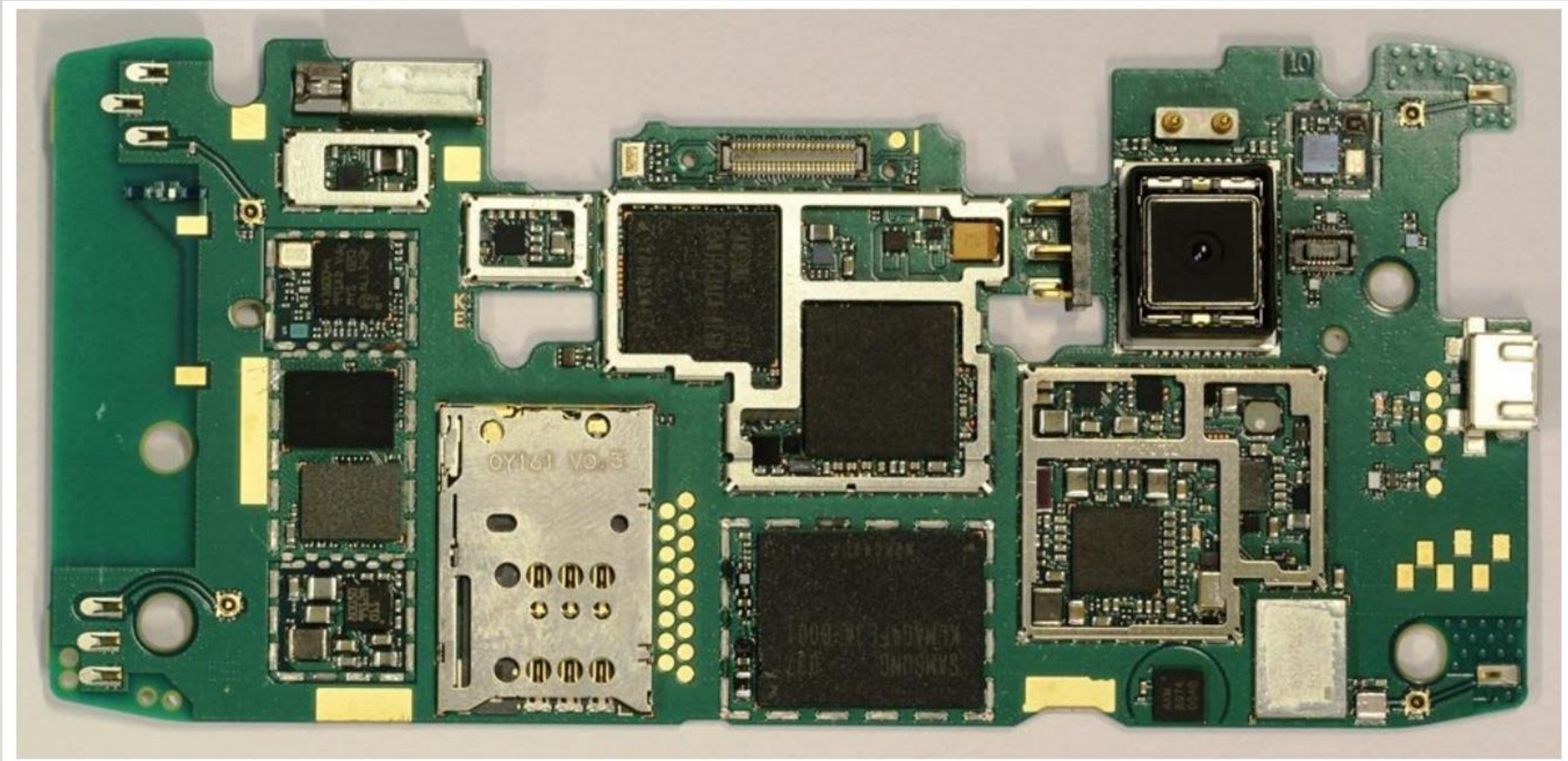
Възможни защити

Възможни защити

- Обновяване на ОС, драйвери и приложения
- Антивирусни продукти
- Защитна стена (firewall)
- Свеждане до необходимия минимум на разпространението на имената на акаунтите за електронна поща и др. услуги

Мобилен телефон

Пример



ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
http://mynokiablog.com/wp-content/uploads/2011/06/n950-insides-5.jpg

Пример

ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
https://mashable.com/2017/02/12/verizon-unlimited-data-is-back/#Nrw4b_LV3Oqz

Възможни защити

Възможни защити (1)

- Криптиране
- Мерки за физическа защита при напускане на охраняемата зона или зоната за сигурност на организацията (респ. на дома) с цел мономизиране на вероятността от кражба или загуба на носителя
- Физическо изтриване на информацията (за flash-базиран носител на информация този вид изтриване не е надежден)
- Създаване на организация за събиране (депониране) на повредена или излязла от употреба електроника, която съдържа носители на информация

Възможни защити (2)

- Обновяване на ОС, драйвери и приложения
- Антивирусни продукти
- Защитна стена (firewall)
- „Надеждна“ парола
- Смяна на парола
- Свеждане до необходимия минимум на разпространението на имената на акаунтите за електронна поща и др. услуги

Закон за електронните съобщения

Закон за електронните съобщения

Закон за електронните съобщения

- Целите на ЗЕС са:
  - да се създадат необходимите условия за развитие на конкуренцията при осъществяване на електронни съобщения
  - да се подпомага развитието на вътрешния пазар на електронни съобщения
  - **да се подкрепят интересите на гражданите като се съдейства за осигуряване на високо ниво на защита на личните данни и неприкосновеността в областта на електронните съобщения**

Закон за електронните съобщения

- В ЗЕС е включен раздел, регламентиращ защитата на данните на потребителите. Според нормите на този раздел, данните на потребителите включват:
  - трафични данни;
  - данни, необходими за изготвяне на абонатните сметки, както и за доказване на тяхната достоверност;
  - данни за местоположението

Закон за електронните съобщения

- Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, съхраняват за срок от 6 месеца данни, създадени или обработени в процеса на тяхната дейност, които са необходими за:
  - проследяване и идентифициране на източника на връзката
  - идентифициране на направлението на връзката;
  - идентифициране на датата, часа и продължителността на връзката
  - идентифициране на типа на връзката
  - идентифициране на крайното електронно съобщително устройство на потребителя или на това, което се представя за негово крайно устройство
  - установяване на идентификатор на ползваните клетки

Закон за електронните съобщения

- Посочените данните се съхраняват за нуждите на националната сигурност и за предотвратяване, разкриване и разследване на тежки престъпления, в това число за целите на предотвратяване на тежки престъпления в рамките на оперативно-издирвателната дейност по реда на глава девета от Закона за противодействие на корупцията и за отнемане на незаконно придобитото имущество
- Други данни, включително разкриващи съдържанието на съобщенията, не могат да бъдат съхранявани по реда на ЗЕС
- Посочените данни се обработват и съхраняват в съответствие с изискванията на Закона за защита на личните данни

Закон за електронните съобщения

- Комисията за защита на личните данни е наблюдаващ орган относно сигурността на данните;
- Като наблюдаващ орган Комисията за защита на личните данни упражнява надзор върху дейността на предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги;
- В случай на нарушение на сигурността на лични данни предприятието, предоставящо обществени електронни съобщителни услуги, уведомява Комисията за защита на личните данни в тридневен срок от установяване на нарушението;

Закон за електронните съобщения

- Когато нарушението може да повлияе неблагоприятно на лични данни или на неприкосновеността на личния живот на абонат или на друго лице, предприятието уведомява своевременно и съответното лице за констатираното нарушение
- Радиосъоръжения и/или крайни електронни съобщителни устройства, включващи хардуерни приспособления към съоръженията или крайните устройства за криптографиране на електронни съобщения и използващи криптографски ключ с дължина, по-голяма от 56 бита, се произвеждат или внасят след регистрация в дирекция "Технически операции" на Държавна агенция "Национална сигурност"

Закон за електронните съобщения

- На лицето, което внася и произвежда такива радиосъоръжения и/или крайни електронни съобщителни устройства, дирекция "Технически операции" на Държавна агенция "Национална сигурност" издава удостоверение за вписването в публичен регистър
- Лица, които извършват сделки с такива радиосъоръжения и/или крайни електронни съобщителни устройства, предоставят писмена информация на Държавна агенция "Национална сигурност" относно всяка сделка с такова съоръжение или устройство - име, тип, сериен номер и идентификационни данни за лицето, с което е осъществена сделката, периодично най-малко на три месеца

ДАННИ ЗА ИДЕНТИФИКАЦИЯ

Част 4

Модифициране на карти за достъп

Цели

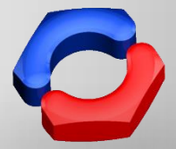
- Нерегламентиран достъп
- Пестене на средства
- Набавяне на средства
- Демонстрация на слабости на системата
- Престиж, удоволствие

Цели

- Ключове
- Тайни (ПИН, пароли и т.н.)
- Критични данни (публични ключове, състояния на жизнения цикъл и т.н.)
- Неоторизирани операции (без да се знаят тайни - например използването на сертифициращ орган)
- Промяна на нормалната работа

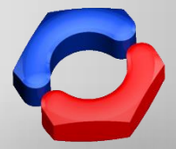
Анализ

- Хардуер
- Софтуер
- Данни
- Жизнен цикъл и взаимодействие между елементите
- Интерфейси на взаимодействие с външния свят



Жизнен цикъл

- Проектиране и разработка на жизнения цикъл
- Производствен жизнен цикъл
- Жизнен цикъл на OS
- Живот (и) на приложение (я)
- Експлоатационен жизнен цикъл



Интереси на атакуващия

- Криминални: с цел финансова печалба (например измама, изнудване)
- Интелектуални: с цел репутация, финансиране или подпомагане на "по-висша" цел или "интелектуално удовлетворение" (забавно)
- Идеологически: с цел да се наруши и / или дискредитира, атакува репутацията на целта

Ресурси на атакуващия

Основният въпрос обаче е:

"С какви **знания**, **умения**, **оборудване** и други **ресурси** разполага?"

Пример

Видове атаки

- Инвазивна
  - Сондиране
  - Модифициране на структури
  - Промяна на поведението на IC (например достъп до тестовия режим)
  - Индукция (предизвикване) на повреди
- Неинвазивна
  - Нежелано изтичане на информация (анализ на мощността, електромагнитни емисии)
  - Проучване на експлоатационната обвивка – среда, интерфейси и др.
- Полуинвазивна – инвазията не е видима
  - лазерна индукция на повреда

Основна структура на атаката

- „Deprocessing“
- Проверка / наблюдение
- Задълбочена инспекция
- Връзка
- Модификация
- Дублиране
- Експлоатация

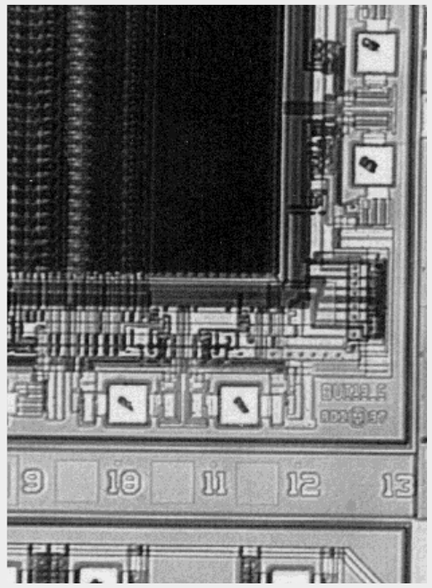
Deprocessing

- Механично
- Химически
- Плазма
- Други

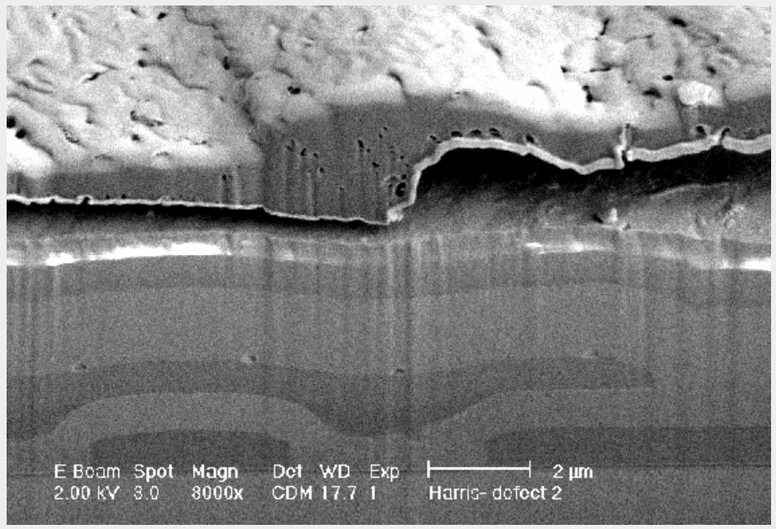
За по-голямата част от инвазивните атаки се изисква deprocessing.

Средства за наблюдение (1)

- Оптичен микроскоп – резолюция 0,18 микрона

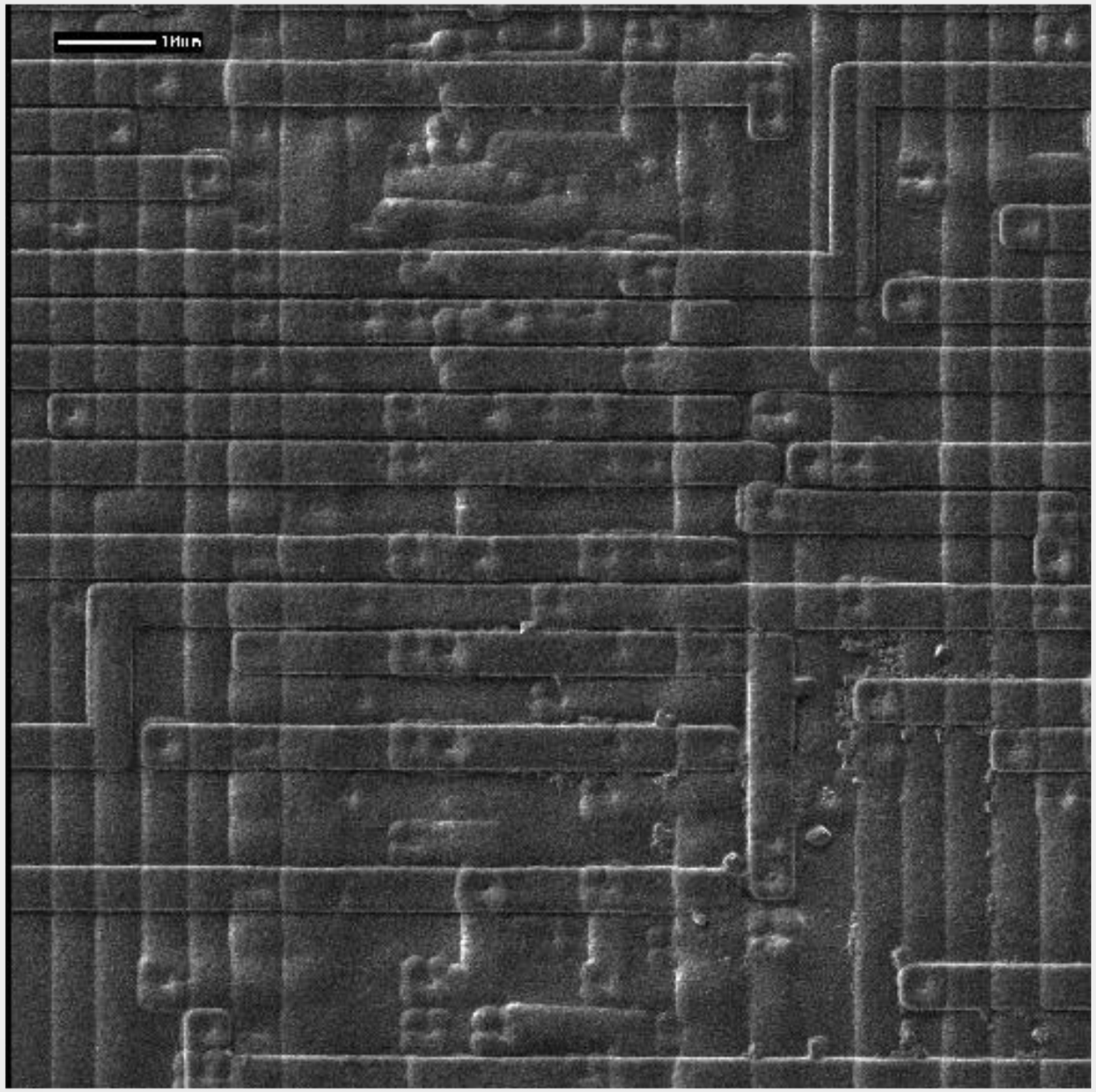


- Електронен микроскоп – резолюция 0,002 микрона



Средства за наблюдение (2)

- Йонен микроскоп – резолюция 0,005 микрона

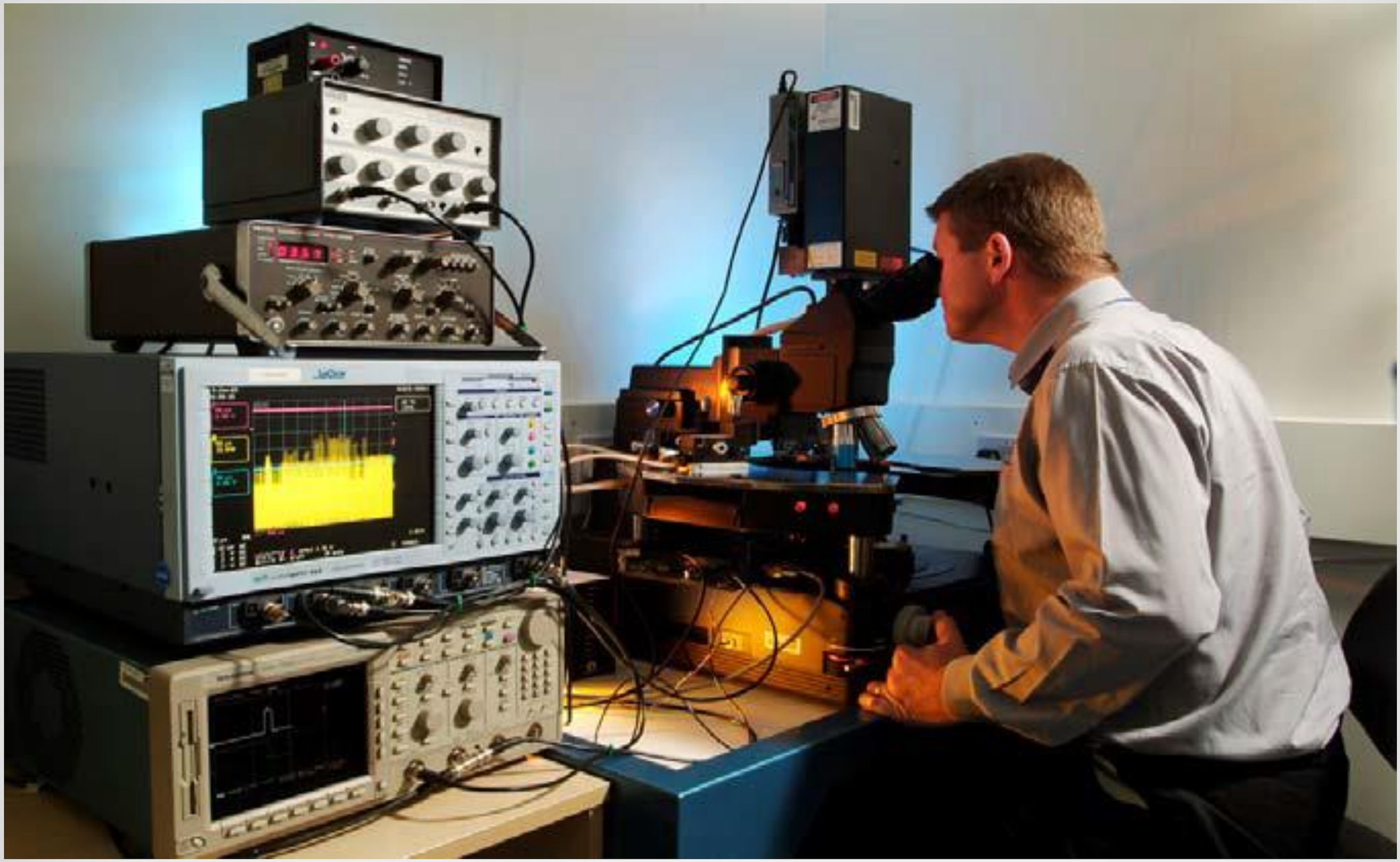


ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
SiVenture, Commercial Product Assurance Test Lab, Великобритания,

Задълбочена инспекция

- Reverse engineering (например използване на инструменти за анализ и симулация на изображения)
- Четене на ROM -памет чрез оцветяване
- Мониторинг на локалните излъчвания

Неинвазивни атаки



ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
SiVenture, Commercial Product Assurance Test Lab, Великобритания

Цената

- Сравнително ниска (под $ 100 000, достъпно оборудване)
- Необходима умерено задълбочена експертиза
- Картата / чипът може да бъде неповредена (или поне да е все още използваема)
- В някои случаи може да се получат данни след няколко секунди ("while-you-wait")

Инвазивни

- Подпомагане на DPA / DFA
- Изрязване на сензори
- Деактивиране или четене на генератор на случайни числа
- Измерване на мощността, където е генерирана (без изкуствен шум)

Цената

- Много ниска (под $ 10 000, достъпно оборудване и инструменти)
- Необходима умерено задълбочена експертиза
- Картата / чипът може да бъде неповредена (или поне да е все още използваема), но е видимо модифицирана
- Сравнително кратко време за работа

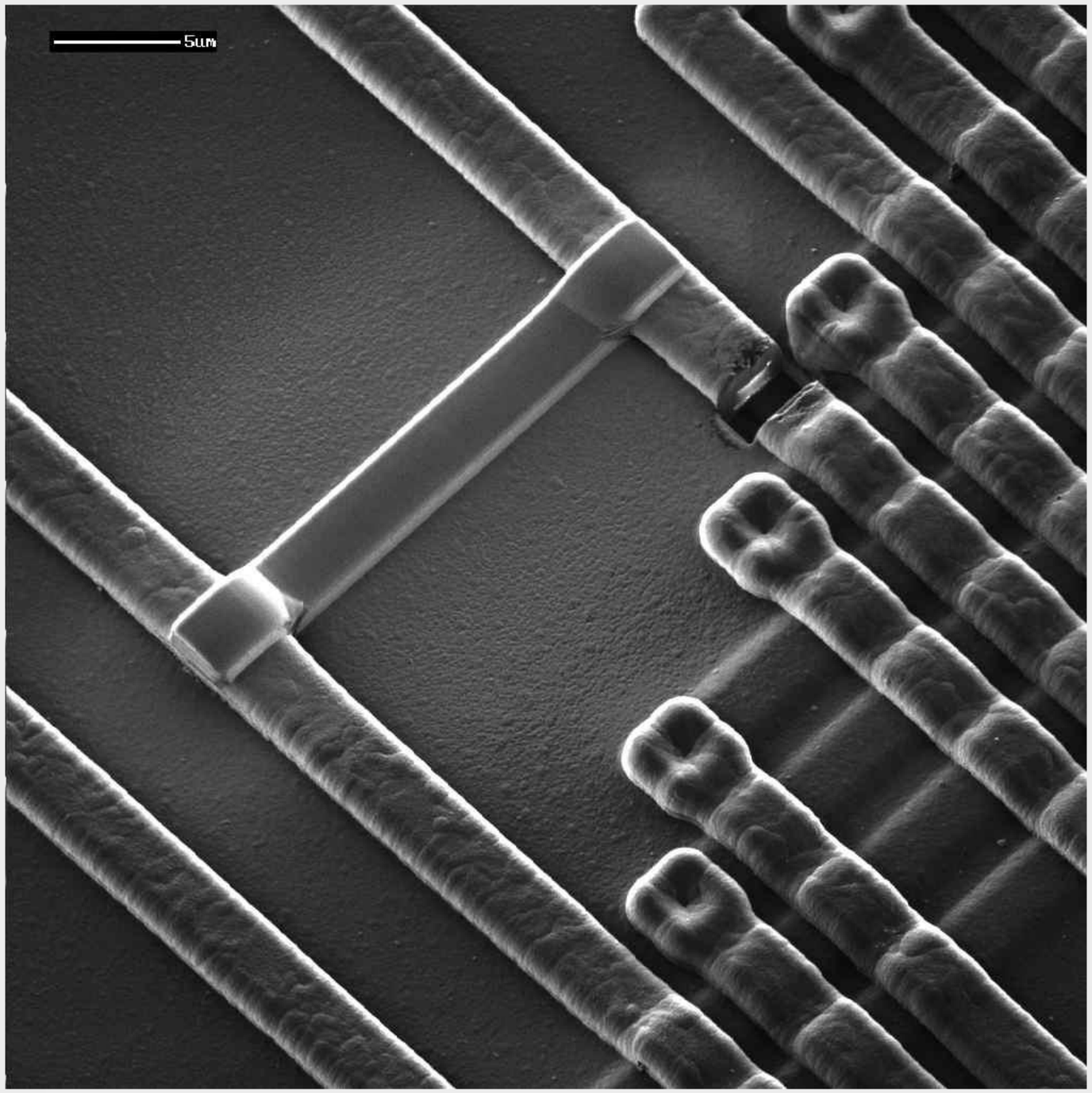
Полуинвазивна

- Подпомагане на DPA / DFA
- Изрязване на сензори
- Деактивиране или четене на генератор на случайни числа
- Измерване на мощността, където е генерирана (без изкуствен шум)

Цената

- Изключително висока (електронен микроскоп, до $ 1 000 000, уникално оборудване)
- Необходима задълбочена експертиза и научно-приложен подход (разработката на микроскопа е плод на два университета)
- Картата / чипът е неразличима на външен вид от оригинала
- Обикновено изисква сравнително дълго време и прецизна работа
- Трайно решение, позволяващо продължителен и задълбочен анализ на цялата система

Генератор на случайни числа



ИЗТОЧНИК НА ИЗОБРАЖЕНИЕТО:
SiVenture, Commercial Product Assurance Test Lab, Великобритания,

Модел на атаки на смарт карти

- Моделът се поддържа от JHAS (JIL Hardware- related Attacks Subgroup), която е част от работната група JIL. Координира се от JIWG = "Joint Interpretations Working group"

https://www.sogis.org/uk/detail_operation_en.html

- Целта на Модела на потенциални атаки е основно за идентифициране на пътища за атака, които се състоят от последователни стъпки на атака, всяка от които има работна функция
- Работните функции за идентифициране на атака могат да се различават от работните функции за нейната експлоатация (напр.: ако даден датчик е открит и прекъснат веднъж, след което може лесно да се повтори на други проби, атаките могат да бъдат сценирани)
- Използва се в процеса на сертифициране по Common Criteria на смарт карти и токени за съхранение на лични данни, цифрови сертификати, контрол на достъпа и др.

Go back to...

- НОВО: Възможност за криптиране на чиповете с технология, която ги прави невъзможни за копиране/клониране!

Препоръки за юридическите лица

Препоръки за юридическите лица

- Вземане на подходящи мерки за сигурност на етапа на проектирането и по подразбиране;
- Обмисляне на възможни мерки за псевдонимизиране, криптиране, анонимизиране на данните;
- Минималните технически мерки могат да бъдат:
  - правилно конфигурирани защитни стени
  - управление на достъпа (чрез User Account Control) – препоръчително е да няма служители с пълен достъп до файловете
  - пароли за достъп
  - редовни актуализации на софтуера
  - антивирусен софтуер за защита в реално време
  - криптиране на всички преносими устройства

Препоръки за юридическите лица

- Минималните организационни мерки могат да бъдат:
  - подписване на споразумения за неразкриване на информация;
  - обучение на персонала във връзка с обработването на лични данни;
  - забрана за използване на личен имейл за работа;
  - ограничаване достъпа на персонала до лични данни до определени лица.

- Минималното ниво на технически и организационни мерки в Република България е регламентирано в Наредба № 1/30.01.2013 г.

Препоръки за юридическите лица

- Анонимизиране ≠ псевдонимизиране
- Разликата между двете понятия се състоя и това, дали личните данни могат да бъдат идентифицирани отново.
- Криптиране – математическа функция, която използва таен ключ за кодиране на данните. Препоръчително е въвеждането на политика, уреждаща използването на криптиране.

Добри практики

ISO

NIST

NIST – National Institute of Standards and Technology

- NIST - Национален институт за стандарти и технологии – метрологична лаборатория, подразделение на Министерство на търговията на САЩ. В периода 1901-1988 г. е носел името Национално бюро за стандарти.

Според NIST

Примери за лични данни:

- Име, като пълно име, моминско име или псевдоним;
- Персонален идентификационен номер, например номер на социална осигуровка, номер на паспорт, номер на шофьорска книжка, идентификационен номер на данъкоплатеца, идентификационен номер на пациента, и номер на финансова сметка или кредитна карта;
- Адресна информация, като уличен адрес или имейл адрес;
- Адрес за интернет протокол (IP) или контрол на достъпа до медиите (MAC);

Според NIST

- Телефонни номера, включително мобилни, бизнес и персонални номера;
- Лични характеристики, включително фотографско изображение (особено на лицето или друга отличителна характеристика), рентгенови снимки, пръстови отпечатъци или друг биометричен образ;
- Информация, идентифицираща лично притежание на собственост, като регистрационен номер на превозното средство;
- Информация за лице, например дата на раждане, място на раждане, раса, религия, тегло, дейности, географски показатели, информация за заетостта, медицинска информация, финансова информация.

BSI стандарти и ръководства

BSI

Publications

The State of IT Security in Germany 2016

The report by the Federal Office for Information Security in Germany (BSI) on the current state of IT security in Germany in 2016 shows the increasing complexity in the level of threat as well as in the associated risks for advancing digitalisation. The report illustrates how information security has become an essential precondition for the success of digitalisation in Germany.

The report provides information on the type and extent of key IT threats and resulting risks. It is based on information analysed by the BSI relating to weaknesses and vulnerabilities in currently used information technology, as well as to attacks on IT systems and networks.

The State of IT Security in Germany 2016 (PDF, 2MB, File is accessible)

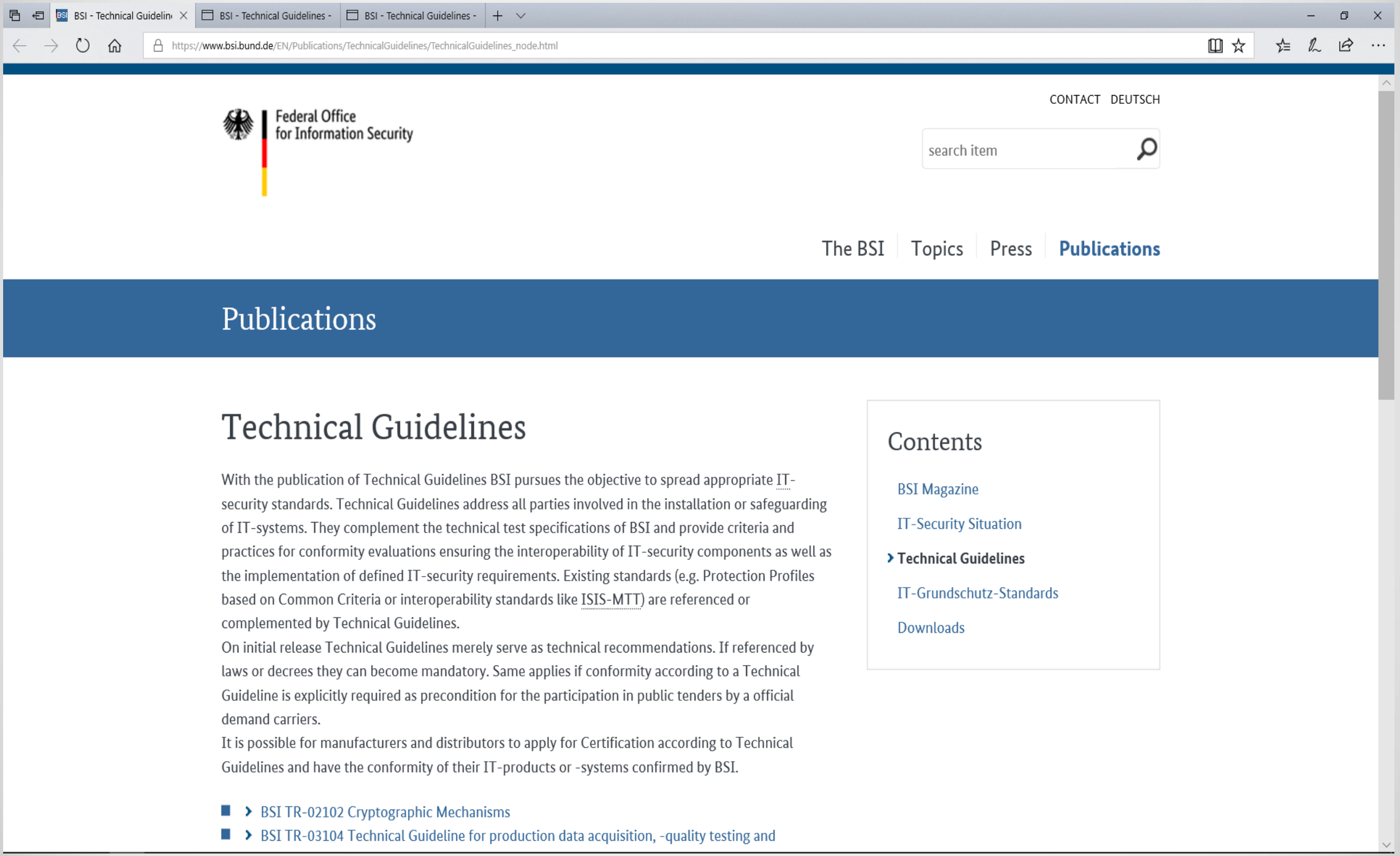
More status reports

- The State of IT Security in Germany 2015 (PDF, 1MB, File is accessible)

BSI - Годишни доклади

- Докладите на Федералната служба за сигурност на информацията в Германия (BSI) относно състоянието на ИТ сигурността в Германия за всяка изминала година показва нарастващата сложност на нивото на заплаха, както и на свързаните с това рискове за напредъка на цифровизацията. Докладите илюстрират как информационната сигурност се превръща в основна предпоставка за успеха на цифровизацията в Германия.
- Докладите предоставят информация за вида и степента на ключовите ИТ заплахи и свързаните с тях рискове. Тя се основава на информация, анализирана от BSI, свързана със слабостите и уязвимостта на използваните в момента информационни технологии, както и с атаките срещу информационните системи и мрежи.

BSI – Технически ръководства



BSI – Технически ръководства

- С Техническите ръководства BSI цели разпространение на подходящи стандарти за ИТ сигурност
- Засягат всички страни, участващи в инсталирането или защитата на информационните системи
- Допълват техническите спецификации и предоставят критерии и практики за оценяване на съответствието, осигуряващи оперативната съвместимост на компонентите на информационната сигурност, както и изпълнението на определени изисквания за ИТ сигурност
- Служат като препоръки
- Ако се споменават от закони или постановления, те могат да станат задължителни. Същото важи, ако съгласно законодателството има предварително условие за участие в обществени поръчки. Възможно е производителите и дистрибуторите да кандидатстват за сертифициране съгласно Техническите ръководства и да получат сертификат за съответствие на техните ИТ продукти или системи с изискванията на BSI.

BSI – Технически ръководства(1)

- **BSI TR-02102** Cryptographic Mechanisms
- **BSI TR-03104** Technical Guideline for production data acquisition, -quality testing and transmission for official documents
- **BSI TR-03105** Conformity Tests for Official Electronic ID Documents
- **BSI TR-03110** eIDAS Token Specification
- **BSI TR-03110** Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token
- **BSI TR-03118** Test Specifications for the Technical Guideline for production data acquisition, -quality testing and transmission for passports
- **BSI TR-03121** Technical Guideline Biometrics for Public Sector Applications
- **BSI TR-03122** Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications

BSI – Технически ръководства (2)

- **BSI TR-03125** Preservation of Evidence of Cryptographically Signed Document V. 1.2
- **BSI TR-03126** Technical Guidelines for the Secure Use of RFID
- **BSI TR-03129** PKIs for Machine Readable Travel Documents-Protocols for the Management of Certificates and CRLs
- **BSI TR-03135** Machine Authentication of MRTDs for Public Sector Applications
- **BSI TR-03137** Optically Verifiable Cryptographic Protection of non-electronic Documents (Digital Seal)
- **BSI TR-03139** Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents issued by EU Member States
- **BSI TR-03140** Conformity assessment according to the satellite data security act (TR-SatDSiG)
- **BSI TR-03145** Secure Certification Authority operation

Криптографски механизми

- **BSI TR-02102-1:** Оценка на сигурността на избрани криптографски механизми. Дава насоки при избора на подходящи криптографски схеми. Документът се отнася основно до разработчиците, които въвеждат нови криптографски защитени инфраструктури.
- **BSI TR-02102-2:** Ръководство за използването на криптографския протокол за сигурност на транспортните слоеве (TLS). Използва се за сигурно предаване на информация в мрежи за данни, като по-специално може да бъде защитена поверителността, целостта и автентичността на предадената информация.
- **BSI TR-02102-3:** Ръководство за използването на криптографски механизми в протоколите IPsec и IKE. Той съдържа само препоръки за версия 2 на протокола IKE (IKEv2).
- **BSI TR-02102-4:** Ръководство за използването на криптографския протокол Secure Shell (SSH) за създаване на защитен канал в несигурна мрежа.

Биометрика в публичния сектор

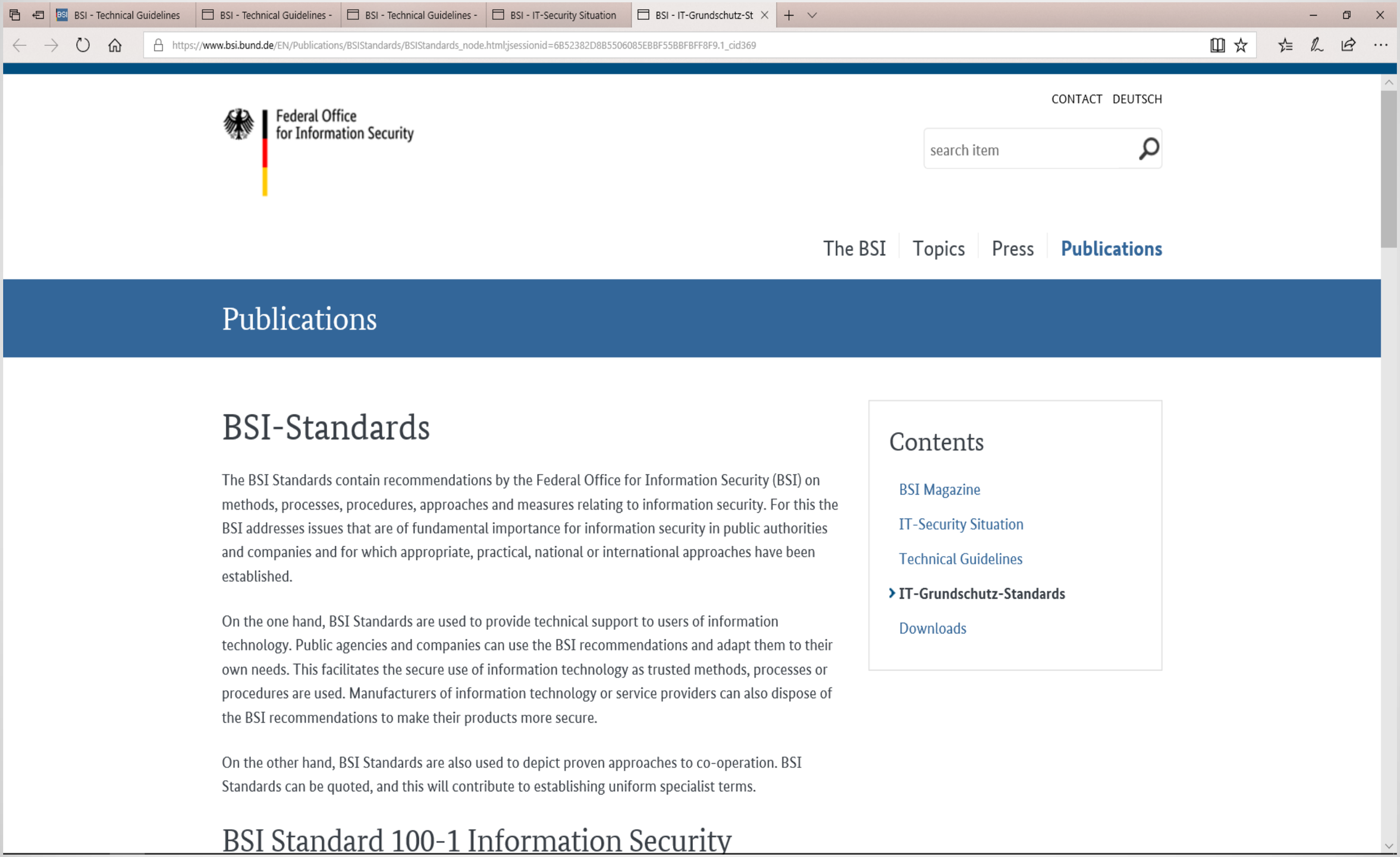
- Използва се в много различни области на обществения сектор, напр. вписването на изображение на лице или пръстови отпечатъци в рамките на прилагането на електронен паспорт или в регистрацията на виза в процесите на граничен контрол за проверка или идентификация на лица
- Решенията и системите, предлагани на пазара, са в състояние да обслужват широк спектър от характеристики, сигурност, използваемост и стандартно съответствие. Поради това за нуждите на публичния сектор е необходимо да се определят точни изисквания и общи условия
- Системите трябва да бъдат дефинирани по начин, който позволява лесни разширения за бъдещи разработки
- Целта на настоящите технически насоки е да се осигури база за последователно и сравнимо качество на приложенията в публичния сектор и за изграждане на обща архитектура

Запазване на доказателства

“Виртуализирането“ на бизнес процесите и документите в електронна форма води до нови предизвикателства, които не съществуват в "стария свят" на хартиените документи - или поне бяха значително по-меки:

- Електронният документ не може да бъде възприет или прочете
- Доказателство за цялост и автентичност и за защита и запазване на правните искове на издателя или на трети лица и доказателство за тяхната точност в електронните правни и стопански сделки
- Необходими са допълнителни технически и организационни мерки, за да се генерират и поддържат тези характеристики в дългосрочен план за целите на дългосрочното съхранение на електронни документи
- Също така и особено в електронния свят, достъпът до данните и документите трябва да отговаря на изискванията за защита на данните и сигурност на данните, дори и за дълги периоди от време и при промяна на системите.

BSI – Стандарти



BSI – Стандарти

- Съдържат препоръки на BSI относно методите, процесите, процедурите, подходите и мерките, свързани с информационната сигурност
- BSI разглежда въпроси, които са от основно значение за информационната сигурност на публичните власти и дружества и за които са установени подходящи, практически, национални или международни подходи
- Използват се за осигуряване на техническа поддръжка на потребителите на информационни технологии. Публичните агенции и дружества могат да използват препоръките и да ги адаптират към собствените си нужди. Производителите на информационни технологии или доставчици на услуги също могат да се разпореждат с препоръките на балансовите показатели, за да направят продуктите си по-сигурни
- Използват се и за описване на доказани подходи за сътрудничество
- Цитирането на стандартите допринася за установяването на единни специализирани условия.

BSI – Стандарти (1)

- **BSI Standard 100-1:** Information Security Management Systems (ISMS): Определя общите изисквания за ISMS. Напълно съвместима със стандарта ISO 27001 и се съобразява с препоръките в ISO стандартите на семейството ISO 2700x. Предоставя лесно разбираеми и систематични инструкции, независимо от методите, които използват.
- **BSI-Standard 100-2:** IT-Grundschutz Methodology: Интерпретира много общите изисквания на семейството ISO 2700x и помага на потребителите да ги прилагат на практика с бележки, опит и примери. Каталозите на IT-Grundschutz обясняват какво трябва да се направи и предоставят много специфична информация как може да изглежда изпълнението (дори на техническо ниво).

BSI – Стандарти (2)

- **BSI-Standard 100-3:** Risk Analysis based on IT-Grundschutz: За потребители на IT-Grundschutz възникват въпроси как трябва да се справят с области, чиито изисквания за сигурност надхвърлят нормалната мярка. BSI предоставя методика за анализ на рисковете, който се основава на IT-Grundschutz. Този подход може да се използва, когато компаниите или публичните власти биха искали да добавят допълнителен анализ на сигурността към анализа IT-Grundschutz.
- **Risk analysis with the new threat catalogue T 0 “Elementary Threats”:** Каталозите на заплахите са от основно значение за използването на методологията (BSI-Standard 100-2) и анализът на риска (BSI-Standard 100-3). Към тях е добавен нов каталог на заплахите T 0 "Елементарни заплахи". Необходимите корекции на методологията за анализ на риска с този каталог са дадени в “Supplement to the BSI-Standard 100-3”.

BSI – Стандарти (3)

- **BSI-Standard 100-4:** Business Continuity Management: Развива систематичен начин за разработване, създаване и поддържане на система за управление на непрекъснатостта на работата на цялата система на една организация, агенция или компания.
  Целта на управлението на непрекъснатостта на бизнеса е да се гарантира, че важните бизнес процеси се прекъсват временно или не се прекъсват изобщо, дори в критични ситуации. За да се гарантира оперативността и следователно оцеляването на компания от индустрията, услугите или държавна агенция, трябва да се вземат подходящи предпазни мерки за повишаване на надеждността и надеждността на бизнес процесите, както и да се даде възможност за бърза и целенасочена реакция в случай на извънредна ситуация или криза.
- За приложение в индустрията са дадени препоръки включително в областта на поддръжката и развитието на технологиите.

BSI – Контакти

https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

ВЪПРОСИ?
ФИНАЛНА ДИСКУСИЯ

Благодарим за вниманието!