PwC Cybersecurity

CyberStrike

https://www.youtube.com/watch?v=prWf9xPqGQs

pwc

Кибер сигурност – рискове

1. Кражба на „чувствителни“ данни (на служителите, клиентите, оперативни, финансови) и интелектуална собственост
2. Прекъсване във функционирането на системите, контролирани от компютри
3. Последствията от хакерска атака:
   - *Риск от загубени клиенти и забавени продажби*
   - *Риск свързан със загубата на репутация*
4. Ние сме „свръх свързани“ (компютри, смарт телефони, интернет, онлайн банкиране, пазаруване и плащания). Колко време прекарвате в интернет…?
5. Несигурен, но достъпен софтуер… пълен с **«бъгове».**
6. Несигурни мрежи и хардуер
   - *Незащитени Wi-Fi*
   - *Системи, изградени от много компоненти = риск*
7. Човешкото поведение
   - *Липса на преценка за ситуацията*
   - *Неяснота как трябва да се държим, когато сме „online“ и „offline“*

Рискове, свързани с клиентите

Опазването на важната информация е задължително!

- **Идентичност -** името на клиента, банковата информация и адресът, на който се изпращат фактурите, трябва да са защитени
- **Данни за транзакциите -** плащанията трябва да са криптирани, а достъпът за извършване на плащания защитен
- **Честота на поръчките -** понякога измамите могат да бъдат замаскирани като изпращане на голям брой малки поръчки, което е нормална бизнес практика и няма да бъдат забелязани
- **Технологии -** лаптопи, смарт телефони, iPads трябва да бъдат защитени с пароли и антивирусен софтуер
- **Социални медии -** голямото количество лична информация, която „post“-ваме може да се използва от хакерите за атака срещу нас или организацията, за която работим

Рискове, свързани със служителите

Какво може да се случи? Няколко примера:

- Толкова много пароли - пароли за лаптоп, десктоп, телефон = „награда“ за вътрешни и външни хакери, които биха използвали паролата Ви, за да направят непозволено плащане
- Изненадващо, но дори не е необходимо да се хакне индивидуален компютър, а представете си ако се хакне мрежовият сървър с принтери (цялата информация, включително и поверителна, която печатате ще е достъпна за хакера)
- Използването на служебни технически средства за лични цели (лаптоп, телефон) позволява свалянето на непроверен/заразен софтуер на служебния компютър
- Важни имейли, които се изпращат от компрометиран имейл адрес (например нареждане за плащане от Директора към Главния Счетоводител)

Рискове, свързани с партньорите

Ние живеем и работим в „свързан свят“…

- Партньорите, с които работите могат да ви изложат на риск:
  - *Outsourcing на счетоводство/HR/плащане на заплати на трети лица*
  - *Обмяна на електронни поръчки/фактури с бизнес партньорите*
  - *Даване на достъп на външни лица до вашата система за поръчки – B2B relations*

- Когато сте част от пазара, съществува риск от:
  - *Изтичане на поверителна информация за участие в търг*
  - *Изтичане на информация за клиентите ви когато ви напусне служител от отдел „Продажби“*
  - *Кражба на интелектуална собственост (договори, информация за цени и отстъпки)*

Да бъдеш хакнат не е въпрос на „дали“, а по-скоро на „кога“

- Експертите смятат, че е време компаниите да приемат пробивите в мрежите си за неизбежни
- Това ще им позволи да променят подхода си в защитата на информация и да постигнат по-реални подобрения
- **Сигурността не се крие в ограничаването на движението на информацията, а в разбирането на това как се движи и споделя**
- Трябва да се прилага подобрен контрол над достъпа (например няколко степени за потвърждение на идентичността)
- Криптирането на информацията както по време на съхранение, така и при пренос през различни мрежи, системи и платформи, подобрението на управлението и съхранението на ключовете за декриптиране са другите важни нови подходи към по-добра сигурност

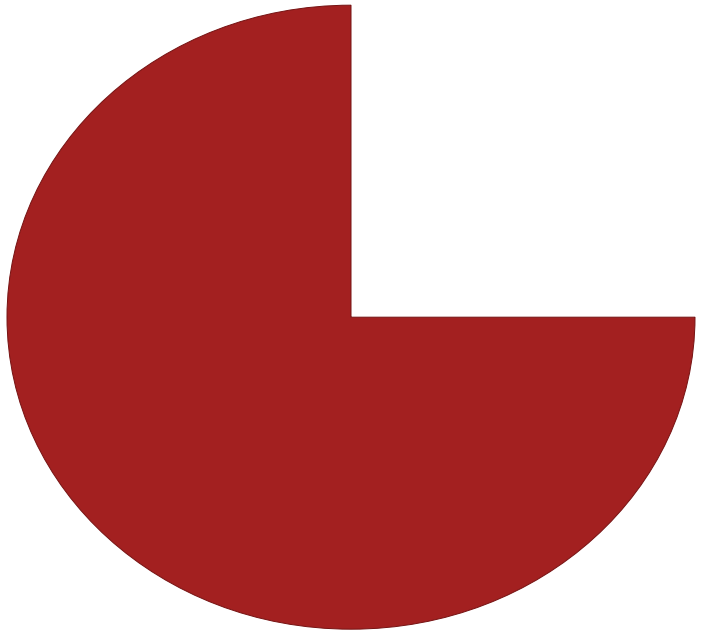
Естеството на атаката

- „Противникът“ ще атакува най-слабата точка на мрежата:
  - *Потребителя*
  - *Веригата на доставки*
- Атаките са много селективни:
  - *Висши мениджъри и служители (достъп до информация)*
  - *Системни и Мрежови Администратори (privileged credentials)*
  - *Доставчици*

- Събирането на наличната „Open source“ информация позволява на атакуващият да се запознае с и да проучи ‚жертвата‘ преди атаката:
  - Организационна структура, технологии, информация на уеб-страница и в социалните медии

- Атакуващият ще предприеме прости методи, за да е успешен:
  - Простите техники позволяват на противника да организира повече атаки (Изискват се по-малко знания и технология)

Статистиката



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Изкуството на войната

Обобщени резултати от +50 симулации на кибер атаки, извършени от екипа на PwC, отговарящ за Cyber Security

Слаба превенция

Получихме **неоторизиран достъп до офиси и сървърни помещения**, където се съхранява и обработва чувствителна информация.

4 часа
е средното време за получаване на достъп до чувствителни данни и/или системи

Получихме **неоторизиран достъп** и/или **контрол** над компютри, сървъри, памет на принтери и скенери.

Не бяхме разкрити

Получихме достъп до **чувствителни бизнес документи**, **пароли** на служители, **банкови/електронни търговски транзакции и информационни системи**.

Успяхме да извлечем данните и да ги изпратим извън мрежата на компанията.

90%
от тестваните организации не откриха/не реагираха на кибератаката

Ниски нива на осведоменост

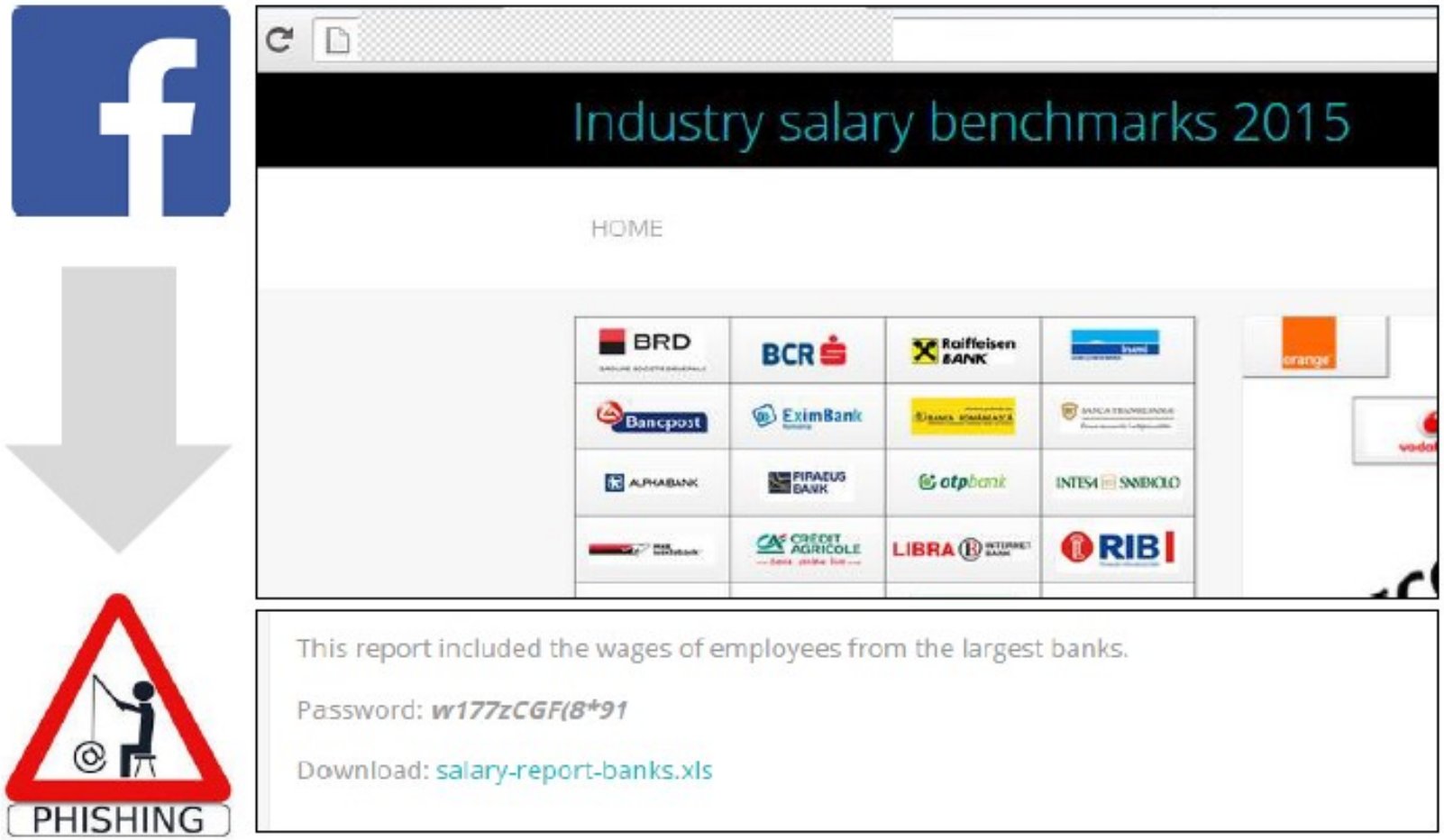
Изградихме фишинг сайтове и успешно насърчихме служителите да **изтеглят заразени файлове.**

100%
от служителите разкриха паролите си в резултат на фишинг тест

Само в един случай служител докладва подозрителни дейности на отговорниците по сигурността.

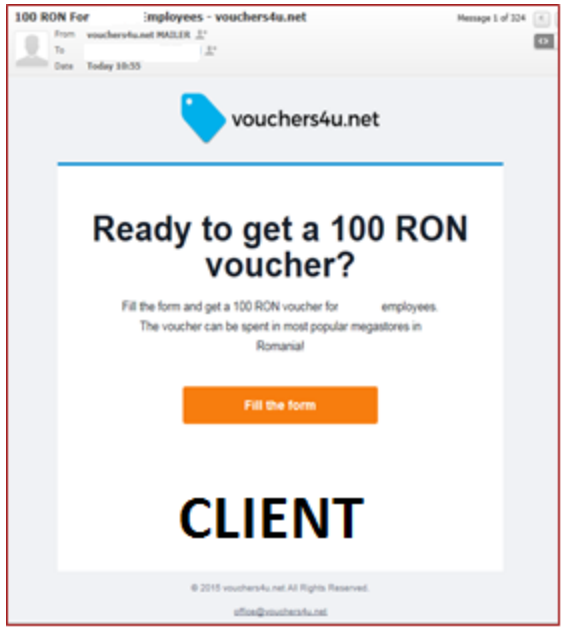
Разузнаването – когато познаваш врага и себе си, изходът от битката е предизвестен

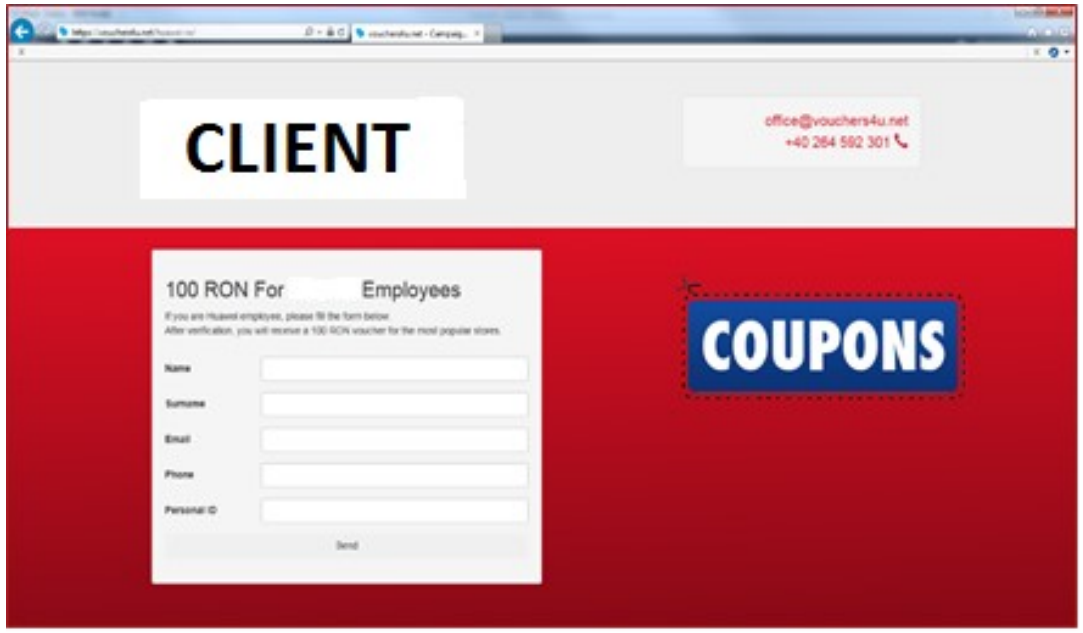
Атаката – в основата на всяка война е заблудата



Атаката – в основата на всяка война е заблудата

Прекалено хубаво е, за да е истина!





Регистрирахме, че 6 служителя са отворили страницата.

Двама от тях са попълнили… личните си данни.

Атаката – в основата на всяка война е заблудата

Hi XXXXXXXX,

I hope this finds you well.

I work within telecommunications market on the permanent side here at topbrains.it.

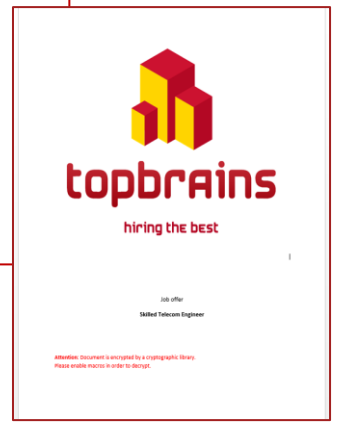
I have a client seeking Skilled XXXXXXXX Engineer based in Romania to work on contract or for permanent position. My client is a fortune 500 company and is a market leader in the XXXXXXXX industry. They have a smooth interview process (initial phone and then face-to-face interview) and offer very competitive salary.

If you would like to see more details on the job specification, please see the attached job offer. I look forward to hearing from you.

Kind Regards,
Greg

--
topbrains.it - hiring the best

Greg Folt
E-mail: greg.folt@topbrains.it
Mobile: +44 7700 900742



3 служителя отварят заразения документ и хакерът получава достъп до компютрите им.

Атаката – в основата на всяка война е заблудата

Dear all,

We are planning to introduce a **new security policy**, which will apply to all employees of CLIENT Global Support Center COUNTRY.

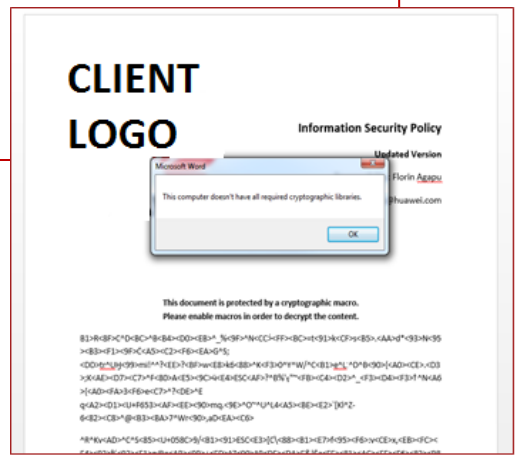
At first, we are going to share the draft of the security policy with a limited number of people just to get your feedback. We would like to know, **if the new regulations won't disturb your daily work activities.**

Please read the attached security policy carefully. Today EoD, you will get an individual link to an online survey, in which you will be able to share your opinion about the document.

Thank you,

Client1 CLIENT2

Program Management Office Department



Един служител отваря документа и ние получаваме достъп до компютъра.

Служителят е част от ИТ екипа на компанията.

И още...

Член на нашия екип в Румъния напуска „restricted client premises“ като част от успешен social engineering пробив.

Регламент за защита на данните (GDPR)

- **Целта** му е да хармонизира защитата на данни в целия Европейски съюз

- **Прилага се** от всички контролери/лицата, обработващи данни на гражданите на ЕС, независимо от това къде се намира седалището на администратора на данни или процесора.

- **Статус:** в сила от 24 май 2016 г.
  - **Ще се прилага от 25 май 2018 г.**

- **Ключови изисквания:**
  1. Изработване на карта за потока на лични данни
  2. Право да бъде забравен
  3. Криптиране на личните данни
  4. Изисквания за докладване на инциденти свързани с личните данни
  5. Минимизиране на личните данни
  6. Преносимост на данните

- **Каква е Вашата кибер стратегия?**

Благодаря!

Илиян Стоянов

PwC | Risk Assurance Solutions | Senior Manager
Office: +359 2 9355 243 | Mobile: +359 895 558 319
Email: ilian.stoianov@bg.pwc.com
PricewaterhouseCoopers Audit OOD
9-11 Maria Louisa Blvd., 1000 Sofia, Bulgaria
http://www.pwc.com/bg