Central Government Audit Service
Ministry of Finance

Тренінг з аудиту інформаційних технологій

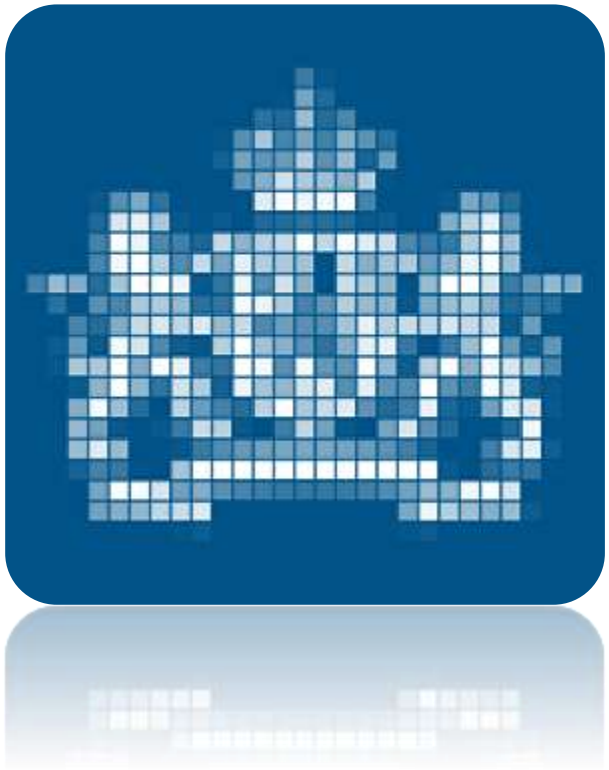
День 3

Рурдьє Просе
Лодевік Янсен

Лютий 2021

Auditdienst Rijk
Ministerie van Financiën

Central Government Audit Service
Ministry of Finance



Порядок денний

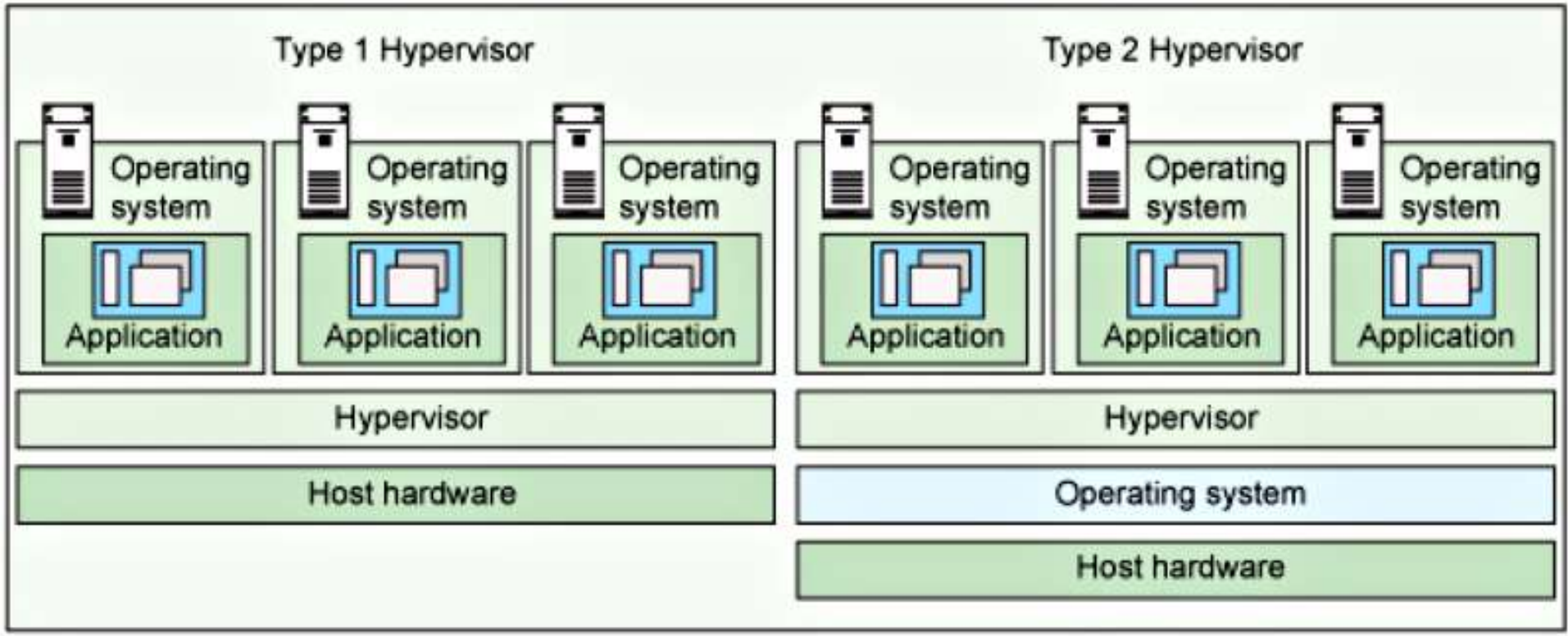
- Обговорення аудиторського підходу
- Представлення кібербезпеки

Хмаринка / віртуалізація

Віртуалізація

Що таке віртуалізація?

https://www.youtube.com/watch?v=GeXwR32GCOw



Хмаринкові технології

Що таке хмаринкові технології:

- Використання послуг з хостингу на інфраструктурі третьої сторони

•Приклади: Webmail, Office 365, Amazon AWS, Azure

• Основоположна хмаринкова інфраструктура така, як мережа, сервери, операційні системи, збереження чи навіть застосунки контролюються і управляються третьою стороною

• Використовує технології віртуалізації та оркестрації для автоматизованого залучення нових серверів, тощо.

Піца як послуга

Традиційна на місці	Інфраструктура як послуга	Платформа як послуга	Програмне забезпечення як послуга
Обідній стіл	Обідній стіл	Обідній стіл	Обідній стіл
Содова	Содова	Содова	Содова
Електрика/газ	Електрика/газ	Електрика/газ	Електрика/газ
Піч	Піч	Піч	Піч
Вогонь	Вогонь	Вогонь	Вогонь
Тісто для піци	Тісто для піци	Тісто для піци	Тісто для піци
Томатний соус	Томатний соус	Томатний соус	Томатний соус
Добавки	Добавки	Добавки	Добавки
Сир	Сир	Сир	Сир
зроблена вдома	напівфабрикат	доставлена піца	вечеря не вдома

Ви управляєте

Продавець управляє

IT підприємства	Інфраструктура	Платформа	Програмне забезпечення
(спадкове IT)	(як послуга)	(як послуга)	(як послуга)
Застосунки	Застосунки	Застосунки	Застосунки
Безпека	Безпека	Безпека	Безпека
Бази даних	Бази даних	Бази даних	Бази даних
Операційні системи	Операційні системи	Операційні системи	Операційні системи
Віртуалізація	Віртуалізація	Віртуалізація	Віртуалізація
Сервери	Сервери	Сервери	Сервери
Місце для збереження	Місце для збереження	Місце для збереження	Місце для збереження
Мережа	Мережа	Мережа	Мережа
Центри даних	Центри даних	Центри даних	Центри даних
	Управляється замовником		Управляється провайдером

Хмаринкові технології

Переваги:

- Швидке і широке застосування / простота реалізації
- Менше власної інфраструктури
- Масштабованість
- Простота оновлення
- Гнучкість
- Низькі затрати
- Простота використання

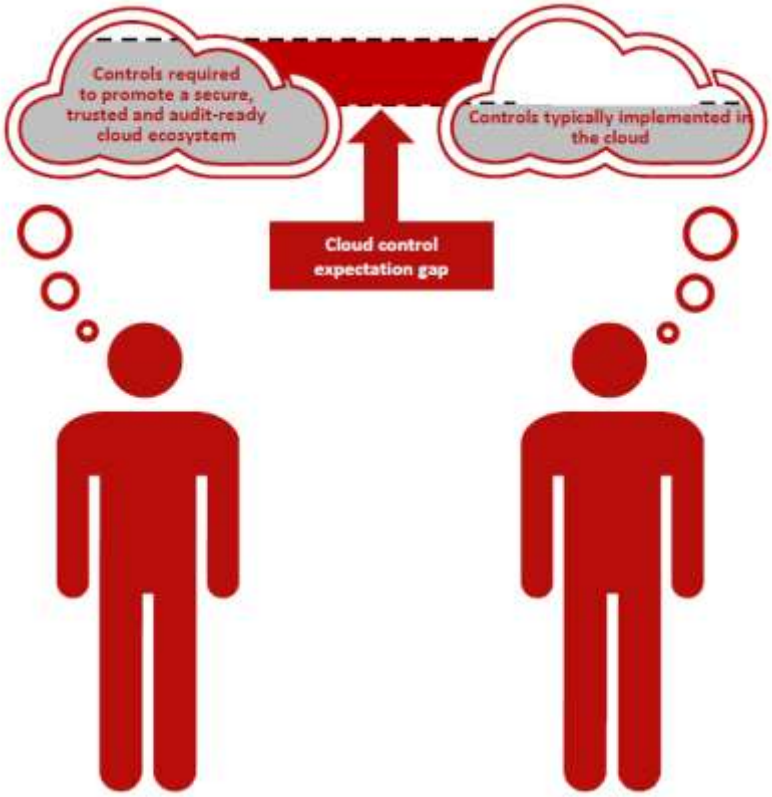
Ризики:

- Безпека даних/конфіденційність
- Відповідність
- Інтеграція з існуючими застосунками / системами
- Управління третьою стороною
- Репутація хмаринкового провайдера

Розрив очікувань щодо хмаринкового контролю

Багато організацій використовують хмаринкові технології

- Клієнти очікують, що постачальники хмаринкових технологій впровадили всі заходи контролю, щоб гарантувати конфіденційність, цілісність, доступність своїх даних
- Насправді: ми бачимо повільніше прийняття необхідних заходів контролю, що здійснюються меншими темпами
- Прогалина між очікуваними заходами контролю та типово запровадженими заходами контролю дедалі більше зростає
- Це ризик для клієнтів хмаринкових технологій



Основи кібербезпеки

Конфіденційність Правдивість Доступність

Конфіденційність:
Захищає вразливу інформацію від перегляду неавторизованими користувачами.
Приклади:

- Фінансові дані
- Номери кредиток
- Номер соцстрахування

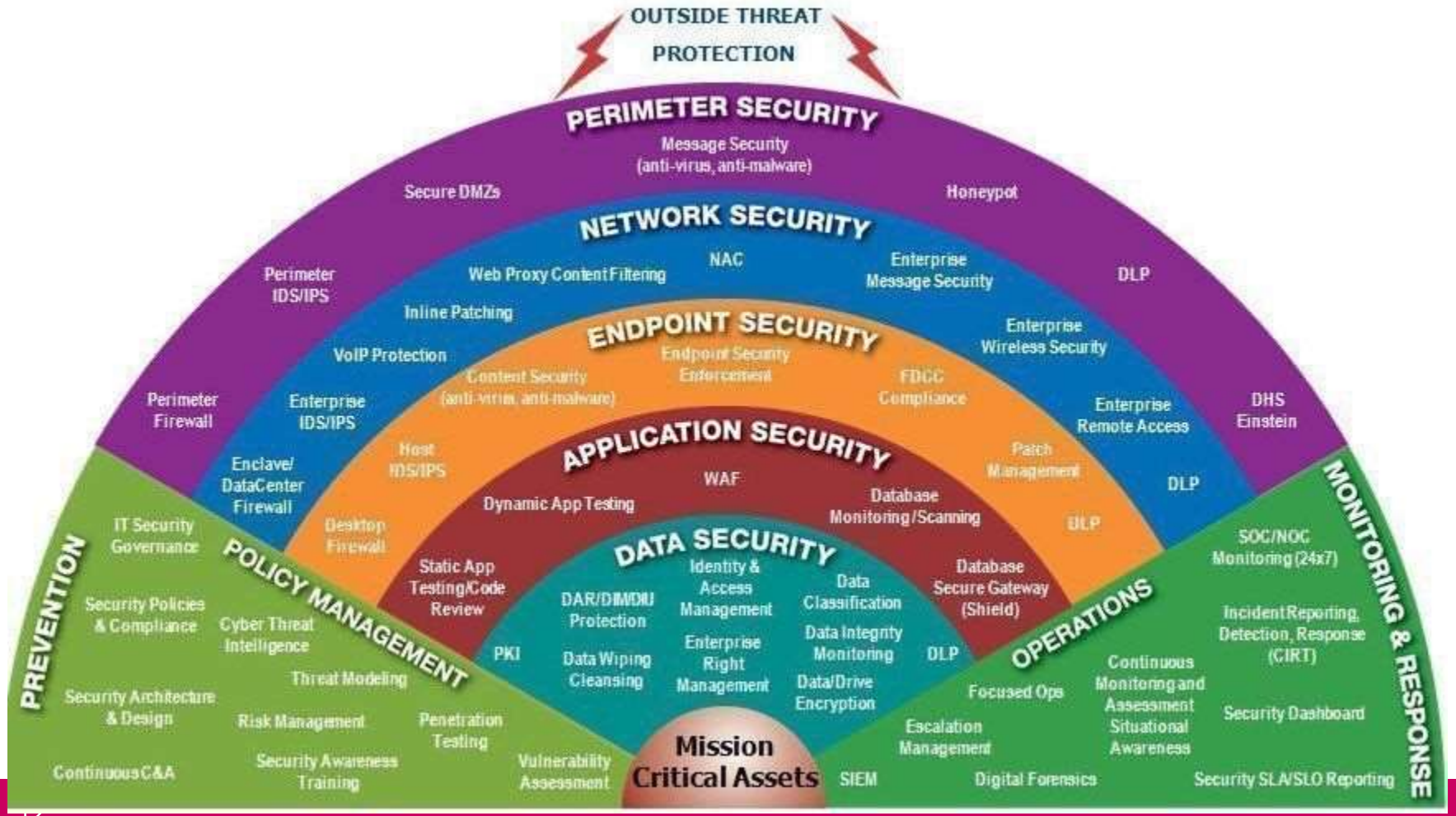
Примітка: Ця ціль прямо пов'язана із внутрішніми і зовнішніми вимогами щодо *Приватності*

Правдивість:
Захищає правдивість вирішальних IT-ресурсів, таких як:

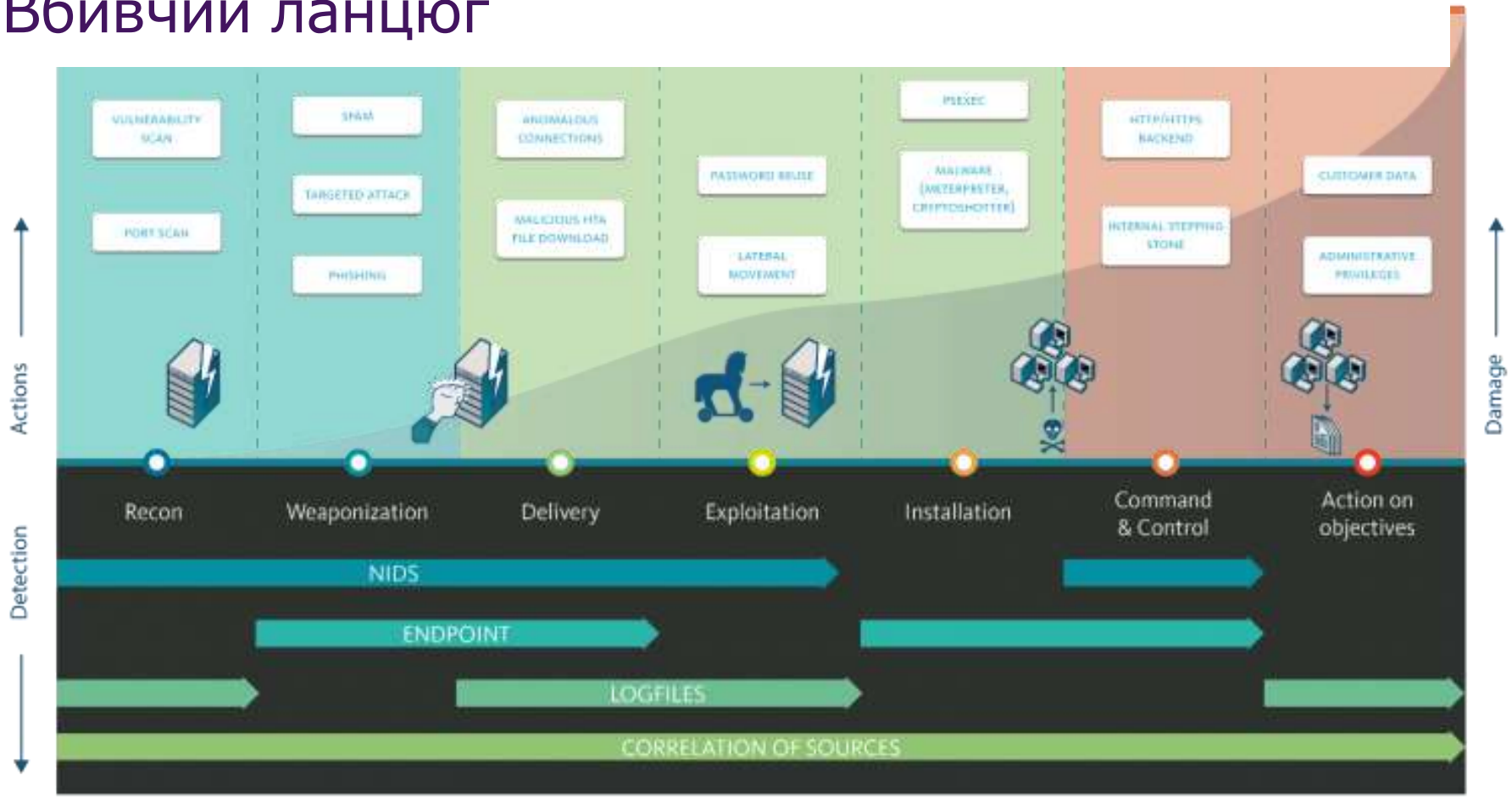
- апаратне забезпечення
- програмне забезпечення
- сховища даних

Доступність:
Забезпечує, щоб вирішальні IT-ресурси (такі як, апаратне і програмне забезпечення, дані) були доступними у потрібний час.

Захист глибинно



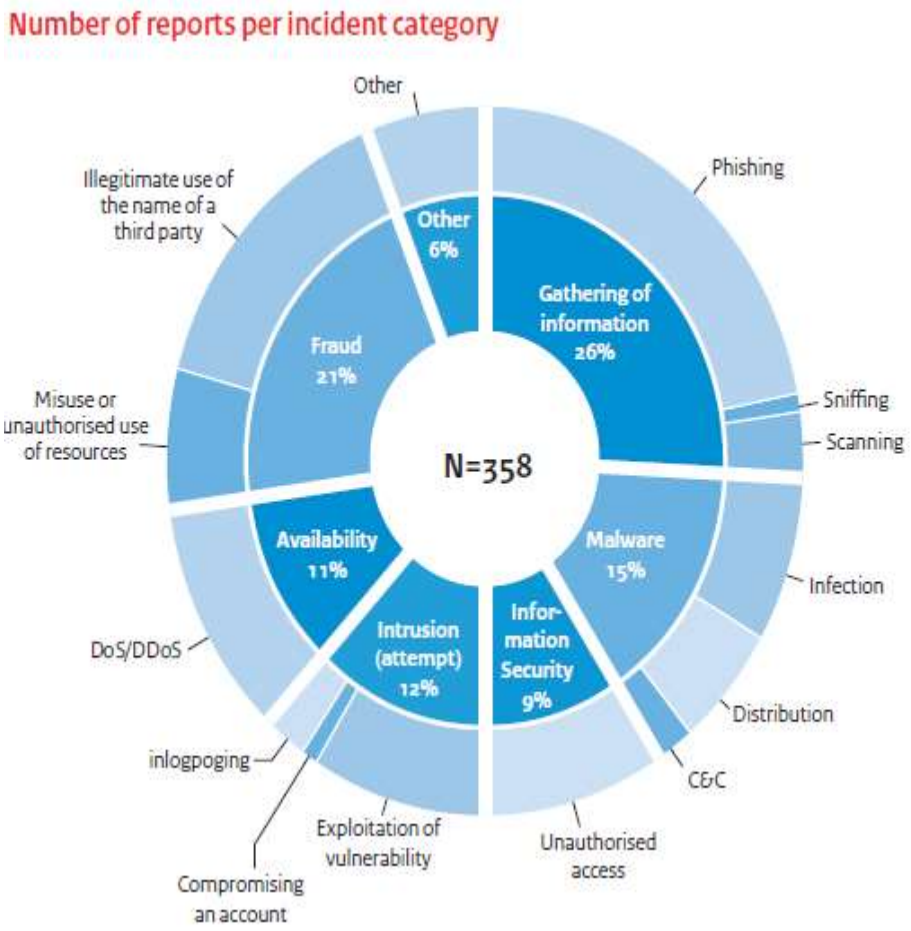
Вбивчий ланцюг



Соціальна інженерія

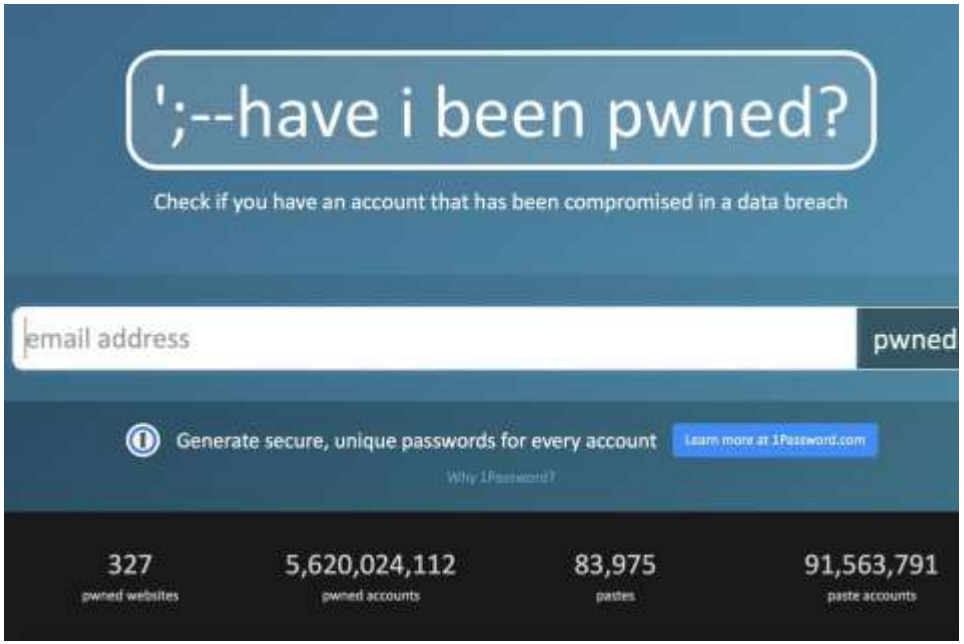
- Фішинг:
- Надсилання емейлів для фішингу
- Клонований електронний лист
- Атака китобою (фішингова атака на топ-персонал)

- Частина майже кожної кібератаки



Характеристики

- Слабкі паролі
- Використання тих самих паролів
- Витік інформації про паролі



Багатофакторна автентифікація (БФА)

- Щось, що ви знаєте (пароль)
- Щось, що ви маєте (токен)
- Щось, ким ви є (біометричне)

- Microsoft: “Ваш пароль не має значення, важлива БФА! На основі наших досліджень, ваш обліковий запис на 99.9% менш вразливий до зламу, якщо ви використовуєте БФА”

96 легко друкується

Password length	Possible Permutations	Time in seconds	Time in minutes	Time in hours	Time in days
6	782,757,789,696	8	0.13	0.002	0.00009
7	75,144,747,810,816	751	12.52	0.21	0.01
8	7,213,895,789,838,340	72,139	1,202.32	20.04	0.83
9	692,533,995,824,480,000	6,925,340	115,422.33	1,923.71	80.15
10	66,483,263,599,150,100,000	664,832,636	11,080,543.93	184,675.73	7,694.82

Бонус: Питання безпеки персональних даних

Можна

Браузер
- Додатки
- Addblock
- Https тільки

Паролі (Keepass)

https://haveibeenpwned.com/

2 фактори автентифікації

Сканування вірусів

Виправлення комп'ютера
- Виправлення комп'ютера
- Оновлення Windows

Обізнаність!

Не можна

Фішинговий електронний лист з гіперпосиланнями на шкідливе програмне забезпечення

Програмне забезпечення для вимагання викупу

Інструмент віддаленого доступу

Ненадійні паролі

Незахищені з'єднання через Wifi

Постійна загроза підвищеної складності