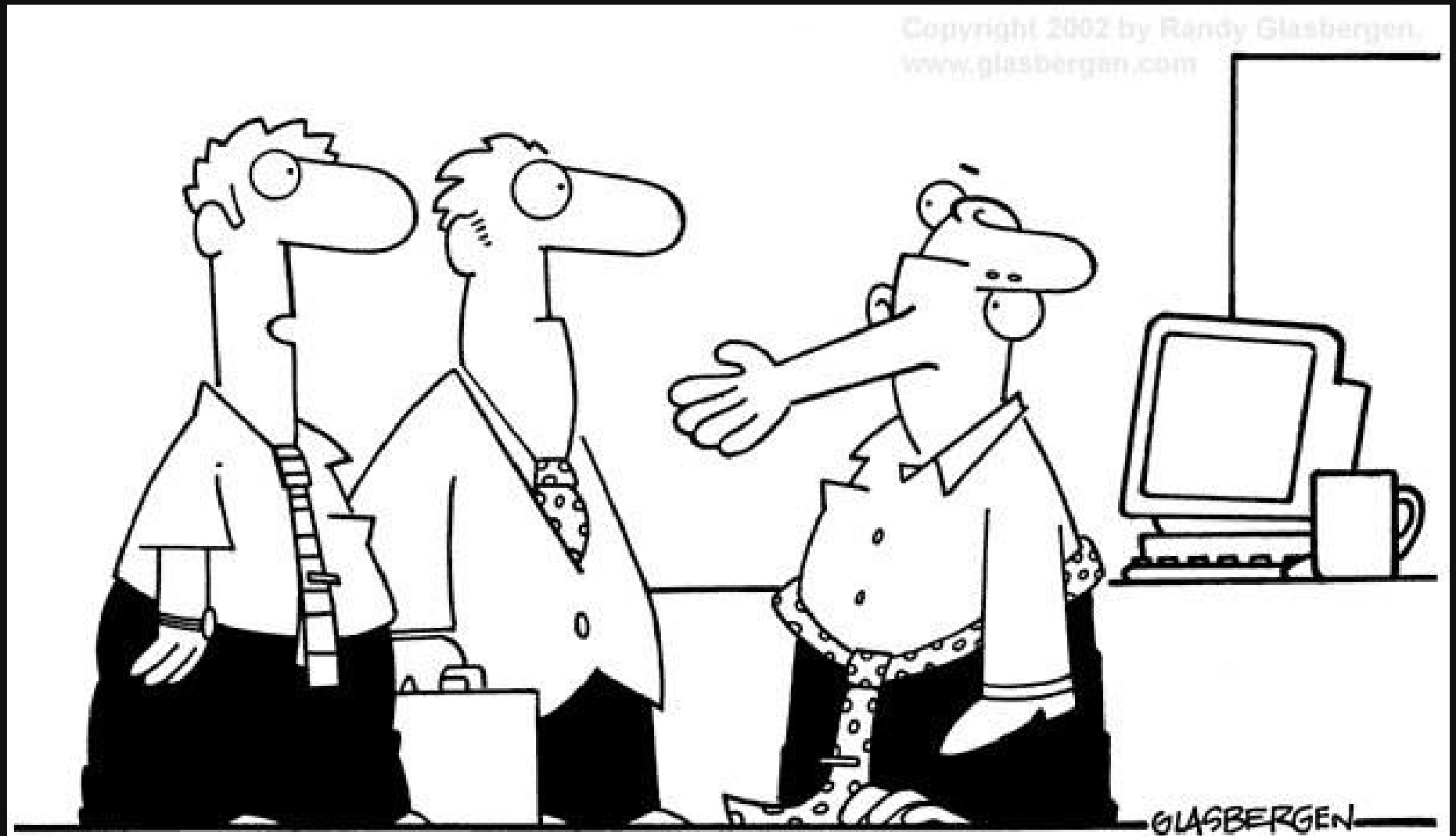
Как же это все произошло?

(c) Игорь Николаев.

Атака на Norsk Hydro. Новое 9/11 мира кибербезопасности



«Это наш ИТ-директор. Он зашифрован в целях безопасности»

19 марта

Фишинговая рассылка днем 19 числа
Необычная активность на серверах компании около полуночи
Блокировка заражения за счет отключения сегментов сети (не до конца сработала)

- Зашифрованы данные на компьютерах с Windows
- под удар не попали телефоны и планшеты с другими ОС

- Поражен ряд производств в Норвегии (плавильные завод) и во Франции
- Неспособность подключиться к основным системам вызвала проблемы на производстве и временные остановки
- Значительная часть данных пока не восстановлена из резервных копий

Правильно:

- Станции энергоснабжения были изолированы от основной сети, поэтому не пострадали.
- Специалисты по безопасности сумели довольно быстро отсоединить от сети плавильные заводы, что позволило тем продолжить работу (хотя часть пришлось перевести в наполовину ручной режим).
- Сотрудники могли нормально взаимодействовать после инцидента
- У Hydro есть резервные архивы, с помощью которых можно восстановить часть зашифрованных данных и продолжить работу.
- У Hydro есть киберстраховка, которая должна покрыть хотя бы часть ущерба от инцидента.

Неправильно:

- сеть не была должным образом сегментирована, в противном случае остановить распространение шифровальщика было бы гораздо проще.
- Установленное Hydro защитное решение не сумело перехватить шифровальщик. Периметр безопасности не включал защиту от шифровальщиков других зловредов.
- Контур промышленной сети не имел специализированных ИБ-решений по защите ICS

Апдейт от 5 апреля

Energy: производство восстановлено и работает

Bauxite & Alumina: производство восстановлено и работает

Primary Metal: производство восстановлено и работает, но ручных операций больше на 30%

Rolled Products: производство восстановлено и работает, но ручных операций больше на 30%

Extruded Solutions: в зависимости от завода
Европа, США – до 90% восстановлено
Строительные подразделения – 75% восстановлено


$40M