БЕЗОПАСНАЯ СРЕДА
ЕЖЕНЕДЕЛЬНАЯ ONLINE-КОНФЕРЕНЦИЯ

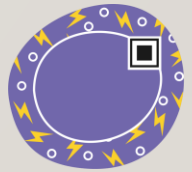
ОТ ХАОСА К ZERO TRUST

ОПЫТ ПРЕОБРАЗОВАНИЯ ИТ-ИНФРАСТРУКТУРЫ НЕСКОЛЬКИХ ЛАТВИЙСКИХ КОМПАНИЙ

PETER GUBAREVICH
MCT, CEH

ВЕКТОРА ДВИЖЕНИЯ

- Australian Cyber Security Centre
  - https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents
- Strategies for Mitigating Advanced Persistent Threats
  - https://encyclopedia.kaspersky.com/knowledge/strategies-for-mitigating-advanced-persistent-threats-apts/
- SANS Top 20 Critical Security Controls
  - https://www.sans.org/blog/cis-controls-v8/



Mitigation Strategy Effectiveness Ranking for 2014 (and 2012)		Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Helps Detect Intrusions	Helps Prevent Intrusion Stage 1: Code Execution	Helps Contain Intrusion Stage 2: Network Propagation	Helps Contain Intrusion Stage 3: Data Exfiltration
1	(1)	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.	Essential	Medium	High	Medium	Yes	Yes	Yes	Yes
2	(2)	**Patch applications** e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.	Essential	Low	High	High	No	Yes	Possible	No
3	(3)	**Patch operating system vulnerabilities**. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.	Essential	Low	Medium	Medium	No	Yes	Possible	No
4	(4)	**Restrict administrative privileges** to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	Low	No	Possible	Yes	No

Once organisations have effectively implemented the Top 4 mitigation strategies, firstly on workstations of users who are most likely to be targeted by cyber intrusions and then on all workstations and servers, additional mitigation strategies can then be selected to address security gaps until an acceptable level of residual risk is reached.

5	(18)	**User application configuration hardening**, disabling: running Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.	Excellent	Medium	Medium	Medium	No	Yes	No	No
6	(N/A)	**Automated dynamic analysis** of email and web content run in a sandbox to detect suspicious behaviour including network traffic, new or modified files, or other configuration changes.	Excellent	Low	Medium	Low	Yes	Yes	No	Possible
7	(21)	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Excellent	Low	Medium	Low	Possible	Yes	Possible	No
8	(11)	**Host-based Intrusion Detection/Prevention System** to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Excellent	Low	Medium	Medium	Yes	Yes	No	Possible
9	(5)	**Disable local administrator accounts** to prevent network propagation using compromised local administrator credentials that are shared by several workstations.	Excellent	Low	Medium	Low	No	No	Yes	No
10	(7)	**Network segmentation and segregation** into security zones to protect sensitive information and critical services such as user authentication by the Microsoft Active Directory service.	Excellent	Low	High	Medium	Yes	No	Yes	Possible
11	(6)	**Multi-factor authentication** especially implemented for remote access, or when the user is about to perform a privileged action or access a sensitive information repository.	Excellent	Medium	High	Medium	No	No	Possible	No
12	(8)	**Software-based application firewall, blocking incoming network traffic** that is malicious or otherwise unauthorised, and denying network traffic by default.	Excellent	Low	Medium	Medium	Yes	Yes	Yes	No
13	(9)	**Software-based application firewall, blocking outgoing network traffic** that is not generated by a whitelisted application, and denying network traffic by default.	Excellent	Medium	Medium	Medium	Yes	No	Yes	Yes
14	(10)	**Non-persistent virtualised sandboxed trusted operating environment**, hosted outside of the organisation's internal network, for risky activities such as web browsing.	Excellent	High	High	Medium	Possible	No	Yes	Possible
15	(12)	**Centralised and time-synchronised logging of successful and failed computer events**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
16	(13)	**Centralised and time-synchronised logging of allowed and blocked network activity**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
17	(14)	**Email content filtering**, allowing only whitelisted business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.	Excellent	High	High	Medium	Yes	Yes	No	Possible
18	(15)	**Web content filtering** of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.	Excellent	Medium	Medium	Medium	Yes	Yes	No	Possible
19	(16)	**Web domain whitelisting for all domains**, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Excellent	High	High	Medium	Yes	Yes	No	Yes
20	(19)	**Block spoofed emails** using Sender ID or Sender Policy Framework (SPF) to check incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organisation's domain.	Excellent	Low	Low	Low	Possible	Yes	No	No
21	(22)	**Workstation and server configuration management** based on a hardened Standard Operating Environment, disabling unneeded/undesired functionality e.g. IPv6, autorun and LanMan.	Good	Medium	Medium	Low	Possible	Yes	Yes	Possible
22	(25)	**Antivirus software using heuristics and automated Internet-based reputation ratings** to check a program's prevalence and its digital signature's trustworthiness prior to execution.	Good	Low	Low	Low	Yes	Yes	No	No
23	(24)	**Deny direct Internet access from workstations** by using an IPv6-capable firewall to force traffic through a split DNS server, an email server, or an authenticated web proxy server.	Good	Low	Low	Low	Yes	Possible	No	Yes
24	(23)	**Server application configuration hardening** e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.	Good	Low	High	Medium	Possible	Yes	No	Possible
25	(27)	**Enforce a strong passphrase policy** covering complexity, length, expiry, and avoiding both passphrase reuse and the use of a single dictionary word.	Good	Medium	Medium	Low	Possible	No	Yes	No
26	(29)	**Removable and portable media control** as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.	Good	High	Medium	Medium	No	Yes	Possible	Yes
27	(28)	**Restrict access to Server Message Block (SMB) and NetBIOS** services running on workstations and on servers where possible.	Good	Low	Medium	Low	No	Yes	Yes	No
28	(20)	**User education** e.g. Internet threats and spear phishing socially engineered emails. Avoid: weak passphrases, passphrase reuse, exposing email addresses, unapproved USB devices.	Good	Medium	High	Medium	Possible	Possible	No	No
29	(26)	**Workstation inspection of Microsoft Office files** for potentially malicious abnormalities e.g. using the Microsoft Office File Validation or Protected View feature.	Good	Low	Low	Low	Possible	Yes	No	No
30	(25)	**Signature-based antivirus software** that primarily relies on up to date signatures to identify malware. Use gateway and desktop antivirus software from different vendors.	Good	Low	Low	Low	Possible	Possible	No	No
31	(30)	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.	Good	Low	Low	Low	No	No	No	No
32	(32)	**Block attempts to access websites by their IP address** instead of by their domain name, e.g. implemented using a web proxy server, to force cyber adversaries to obtain a domain name.	Average	Low	Low	Low	Yes	Yes	No	Yes
33	(33)	**Network-based Intrusion Detection/Prevention System** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Average	Low	High	High	Possible	Possible	Possible	Possible
34	(34)	**Gateway blacklisting** to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.	Average	Low	Low	High	Possible	Yes	No	Yes
35	(35)	**Capture network traffic** to/from internal critical asset workstations and servers as well as traffic traversing the network perimeter, to perform post-intrusion analysis.	Average	Low	High	Low	No	No	No	No

НАПРАВЛЕНИЯ ПРЕОБРАЗОВАНИЙ ИНФРАСТРУКТУРЫ

- Реализация принципа Least Privilege во всех производственных системах
- Контролируемая среда установки ОС и приложений (Application Deployment)
- Контролируемая среда обновлений систем и приложений (Windows Update)
- Реализация Application Whitelisting на всех компьютерах компании
- Обеспечение надёжного резервирования данных
- Трансформация пространства IPv4

ПРЕДПРИНЯТЫЕ ШАГИ: ACTIVE DIRECTORY

- Упорядочивание учётных записей пользователей, администраторов и внешней поддержки.
  Тотальная персональная идентификация субъектов безопасности (нет «админ2», «тест», «поддержка_1С»)
  Включение двухфакторной аутентификации (смарт-карты для администраторов, Push-уведомления для RDP)
- Реструктуризация AD с целью делегирования полномочий сотрудникам ИТ (и не только)
  Разнесение учётных записей компьютеров, пользователей и групп по иерархии контейнеров
  Делегирование требуемого уровня полномочий на нужные контейнеры соответствующему персоналу
  Создание системы авторизации доступа пользователей и компьютеров через членство в группах
- Завязка внешних систем на AD-аутентификацию
  Тотальная централизация идентификации/аутентификации через LDAP (Linux Mail, VPN, Printers etc)
  Ликвидация локальных учётных записей в производственных системах

ПРЕДПРИНЯТЫЕ ШАГИ: РАБОЧИЕ СТАНЦИИ И СЕТЬ

- Внедрение системы распространения и обновления приложений через доменные группы (WSUS)
  Стандартизация образов рабочих станций (WDS), запрет на использование USB сотрудниками ИТ
  Распространение политики Application Whitelisting на все компьютеры
  Включение Bitlocker на всех мобильных компьютерах, гипервизорах и рабочих станциях ИТ
  Отсылка почтовых уведомлений о наиболее важных событиях в журнале Security

- Создание единого IPv4-пространства для всех подразделений компании
  Разделение устройств по VLAN-ам согласно функционалу (принтеры, сервера, сенсоры)
  Изоляция производственных компьютеров (реакторы, SCADA-системы)
  Аутентификация и классификация доступов к VPN, Wi-Fi, Internet через доменные группы
  Внедрение видимости устройств и элементов сети (Dude, Zabbix)

ПРЕДПРИНЯТЫЕ ШАГИ: ДАННЫЕ

- Понятия «держатель процесса» и «держатель ресурса» для общих папок и всех производственных систем
  Централизация совместных проектов и персональных документов пользователей на файл-серверах
  Контроль доступа к общим папкам через доменные группы, делегированные держателям процесса
  Шифрование персональных документов на всех мобильных компьютерах (Work Folders Encryption)
  Теневое копирование всех файл-серверов и рабочих станций, построение системы регулярного бэкапа

- Замена Linux-почты на интегрированный с AD Exchange
  Частичная интеграция с сервисами O365
  Введение принципа архивации почты ушедших сотрудников
  Установка стороннего коммерческого спам-фильтра
  Ликвидация квот и PST-файлов

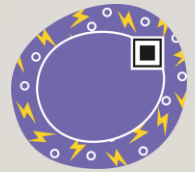
EPIC FAIL SECTION

До Zero Trust нам — как до Луны

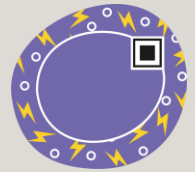
- Преобразования не оформлялись документально Нет политик, правил; не проводилось обучение пользователей.
- Deep Inspection руководство запретило Видимо, опасались за некоторые свои данные.
- Недоверие ряда департаментов сотрудникам ИТ. Одни прячут документы на съёмные носители, другие поднимают крик «мои файлы украдены!»
- Пытаясь объять необъятное, я утонул в оперативных задачах. Оказывается, никто другой не собирается читать отчёты бэкапа и что-то исправлять.
- Далеко не все важные для компании поставщики готовы к сотрудничеству для преобразования своих систем.

LESSONS LEARNED

ЧТО ЯВЛЯЕТСЯ ДРАЙВЕРОМ ПРЕОБРАЗОВАНИЙ? ПОЧЕМУ ЧТО-ТО НЕ ПОЛУЧАЕТСЯ?

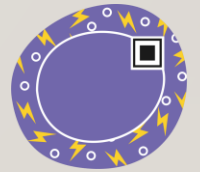


- Успех (или неудача) реализации проектов ИБ, как правило, зависит от одного конкретного человека. Не от имени или размера компании, а от воли, видения, понимания миссии одного человека.
- Без полной поддержки руководства на всех уровнях большинство проектов не будет реализовано. ИБ по сути своей — это ограничения. Обиженные будут жаловаться и пытаться обойти ограничения.
- Для реализации любых проектов ИБ потребуются человеко-часы сотрудников разного уровня. При этом внутри компании должен быть держатель процесса, способный взять на себя все сложные вопросы.
- Многим мероприятиям ИБ нужна культурная готовность компании. Технические решения не могут полностью закрыть проблемы человеческого фактора, а безопасность — это дисциплина каждый день.
- Security Manager не заменяет собой Security Engineer-а, и наоборот. Первый ведёт диалог с бизнесом и классифицирует документы, второй читает журналы аудита и реализовывает конфигурацию IPSec.
- Продуктовые решения должны упрощать существующие процессы, а не пытаться порождать их. Если таковых процессов нет, продукт будет заброшен.



РЕКОМЕНДАЦИИ

А ВЫ УЖЕ УМЕЕТЕ КОРРЕКТНО ПОДСЧИТЫВАТЬ TCO+ROI СВОИХ РЕШЕНИЙ?



- Все ограничения и настройки в первую очередь испытывайте на себе и на ИТ-отделе.
  Например, ИТ не сможет решать проблемы с MultiFactor Authentication, если они это никогда не видели.
- Начинайте внедрять безопасность с наиболее простых участков сети, постепенно наращивая сложность.
  При этом не теряйте времени, пытаясь довести всё до идеала — многие проекты можно считать успешно завершёнными при достижении 95% покрытия.
- Представьте сотрудникам безопасные решения как более удобные, научите работать более эффективно,
  и им не захочется обходить ограничения или выискивать нелегальные пути решения своих задач.
- Делегируйте, делегируйте, делегируйте. Пусть держатели процесса сами решают, какие доступы кому предоставить; ITSec при этом направляет, советует и обучает, разделяя ответственность.
- Автоматизируйте всё, что разумно. Например, сконфигурируйте подключение принтеров через GPO,
  и больше не придётся бороться с ручной инсталляцией заражённых драйверов.