AXOFT
Глобальный сервисный IT-дистрибутор

Zero Trust:
не верь, не бойся, не проси

Евгений Питолин
Управляющий директор

Центральная Азия, страны СНГ и Балтии

kaspersky

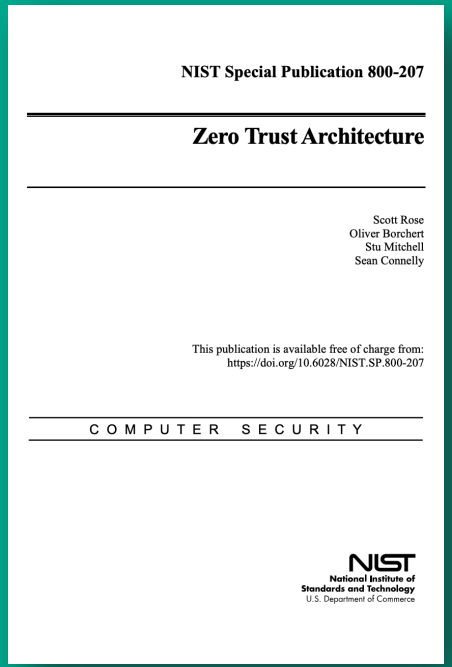
Идем к концепции «Нулевого доверия»

В 2010 году аналитик проекта Forrester Research Джон Киндерваг (John Kindervag) выдвинул концепцию «нулевого доверия» как альтернативу «защите периметра». Он предложил отказаться от разделения ресурсов на внешние и внутренние.

Концепция Zero Trust — это полное отсутствие каких-либо доверенных зон.

В рамках этой модели пользователи, устройства и приложения подлежат проверке каждый раз, когда требуют доступ к какому-либо корпоративному ресурсу

Нулевое доверие по NIST



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

1. Вся частная сеть организации считается НЕ доверенной зоной
2. Устройства в сети могут НЕ принадлежать организации и НЕ конфигурироваться ей
3. Ни один ресурс НЕ является доверенным
4. НЕ все ресурсы организации находятся в корпоративной инфраструктуре
5. Удаленные субъекты и активы организации НЕ могут полностью доверять своему подключению к локальной сети
6. Активы и потоки информации, перемещающиеся между корпоративной и внекорпоративной инфраструктурой, должны соответствовать согласованной политике и принципам информационной бзеопасности

Нулевое доверие и контроль

IDENTIFY (Выявление)	Управление активами (ID.AM) Оценка риска (ID.RA)
PROTECT (Защита)	Управление идентификацией, аутентификация и контроль доступа (PR.AC) Безопасность данных (PR.DS) Процессы и процедуры защиты информации (PR.IP) Технология защиты (PR.PT)
DETECT (Обнаружение)	Аномалии и События (DE.AE) Непрерывный мониторинг безопасности (DE.CM) Процессы обнаружения (DE.DP)
RESPOND (Реагирование)	Смягчение последствий (RS.MI)

Концепция «Нулевого доверия» правильная, но сразу ее реализовать не просто.

К этому обычно не готовы ни системы, ни процессы, ни люди...

Проектируемая безопасность и безопасность по умолчанию

- Проще и правильнее начать с внедрения подхода «Проектируемая безопасность и безопасность по умолчанию» (Security by design and by default (SbDD).
- За основу стоит взять аналогичный подход из защиты персональных данных (Data protection by design and by default (DPbDD)), расширив его до защиты любой ценной информации в компании.

Принципы концепции

1. Превентивные (проактивные) меры, а не только устранение последствий	Внедрение мер защиты соразмерных рискам
2. Безопасность по умолчанию	Внедрение политики «безопасность по умолчанию», в том числе за счет минимизации доступа и внедрения других принципов разграничения доступа
3. Встроенная безопасность	Использование методов безопасной разработки
4. Обоюдная польза	Принятие всех заинтересованных сторон и разрешение конфликтов, исходя из концепции «выиграл-выиграл»
5. Комплексная безопасность на протяжении всего цикла	Комплексное обеспечение конфиденциальности, целостности и доступности информации
6. Наглядность и Прозрачность	Усиление безопасности за счет открытых стандартов, известных процессов и внешнего аудита / контроля
7. Уважение к Пользователю	Уважение и защита интересов всех владельцев информации.

Проектируемая безопасность и безопасность по умолчанию

Типовые меры проектируемой безопасности

- Система управления ИБ (СУИБ)
- Управление рисками
- Техническое обслуживание
- Управление доступом
- Безопасная передача данных
- Безопасное хранение
- Псевдонимизация
- Шифрование
- Резервное копирование
- Управление логами и мониторинг
- Управление инцидентами
- Управление непрерывностью

Принципы управления доступом при проектировании новых систем

1. Принцип наименьших привилегий / Least Privilege
2. Принцип «Необходимо знать» (Принцип «служебной необходимости) / Need-To-Know
3. Принцип наименьшего доверия / Least Trust
4. Принцип Мандатного управления доступом / Mandatory Access Control
5. Принцип разграничения полномочий / Segregation of Duties

Чем хороша концепция «Проектируемой безопасность и безопасность по умолчанию»?

- Общая идея проста: «При проектировании и внедрении процессов и систем сразу задумайтесь о безопасности»
- Внедрение мер ИБ на ранних стадиях существенно дешевле…
- Внедрение концепции – показатель зрелой культуры безопасности в компании
- В основе лежат известные базовые принципы: адекватность ИБ рискам, контроль эффективности и постоянное совершенствование ИБ…

CISO 2021
- апгрейд версии.

Мотивация других людей

практически никто не готов реально нести ответственность за свои «хочу», «мне так удобно» или «и так сойдет».

должен существовать какой-то волшебник, который защитит от всего, какими бы ни были условия.

Персоналу – нужно осознавать свою ИБ-роль и свою ответственность, не перекладывая ее на ИТ/ИБ и руководство.

CISO 2021

Пропадает привкус «товарища майора»

Меняются навыки плаща и кинжала

Долгий и сложный путь от

«Вам нельзя....»

до...
«как сделать так, чтобы Вам было удобно и безопасно работать?»


Поезд
ушёл

ВСЕ БУДЕТ ХОРОШО!

ВСЕ БУДЕТ ХОРОШО!

*даже если вы этого пока не хотите:)

AXOFT
Глобальный сервисный IT-дистрибутор

Будьте здоровы, берегите себя!

Евгений Питолин
Управляющий директор

Центральная Азия, страны СНГ и Балтии

Evgeny Pitolin
Managing Director

Central Asia, CIS & Baltics

kaspersky