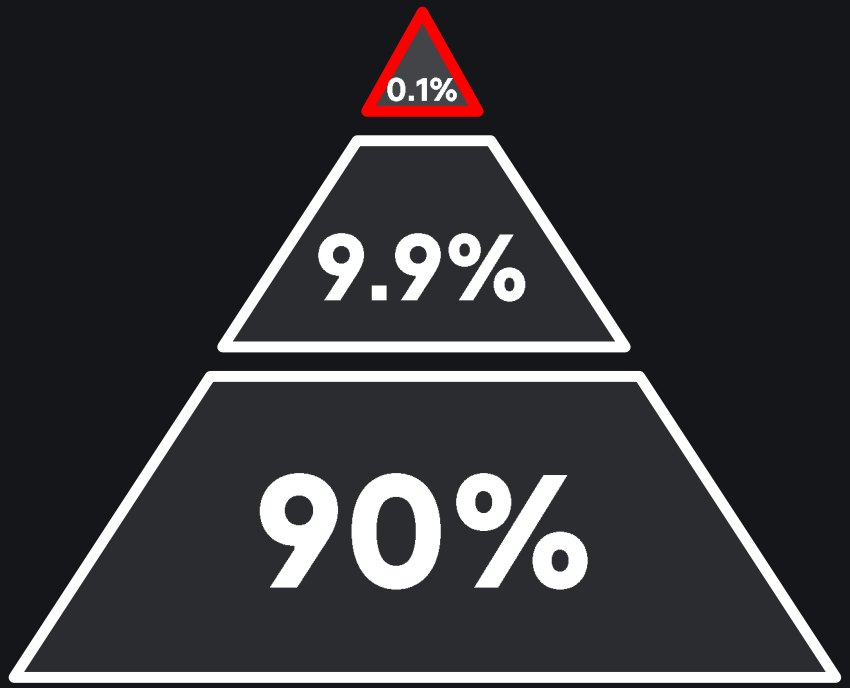
Защищённость корпоративных систем.
Кто виноват (или что)?
Что делать?

Kaspersky

360 000+

Новых угроз обнаруживает «Лаборатория Касперского» **ежедневно**

Ландшафт угроз



Кибероружие

Целевые атаки
на организации

Традиционная
киберпреступность

КАК???

Фишинг

Сокрытие факта проникновения и присутствия в системе

Компрометация учётной записи администратора (домена)

Активное распространение

Поиск и кража данных

Ну как-то вот так!...

Кто виноват (или что)?

- устаревшие (снятые с поддержки) версии ОС (Microsoft Windows) и офисных пакетов (Microsoft Office), а также нерегулярные обновления;
- недостатки в конфигурации средств защиты (возможно, привнесённые злоумышленниками), в том числе нестойкая парольная политика;
- несоблюдение «Принципа минимальных привилегий» (большое количество учётных записей с правами администратора, отсутствие практики использования непривилегированных учётных записей для повседневной работы);
- недостаточная сетевая сегментация и наличие доверительных отношений между доменами;
- недостаточная осведомлённость пользователей по вопросам информационной безопасности

Что делать?!!!

- **<u>РЕГУЛЯРНО РАБОТАТЬ С ПОЛЬЗОВАТЕЛЯМИ</u>!!!**
- активно внедрять и использовать узловые СЗИ с централизованным управлением, регулярно обновлять базы угроз, периодически контролировать настройки СЗИ (запрет их отключения и т.д.) и осуществлять полное сканирование узлов сети;
- разработать политику обновления ПО и выполнять её (предусмотреть регулярные обновления ОС и ПО до версий, находящихся на поддержке производителя, проверку обновлений, устанавливать актуальные обновления безопасности (патчи));
- ограничить права пользователей в соответствии с принципами минимальной необходимости и «запрещено всё, что явно не разрешено»

Что делать?!!! (часть 2-я)

- для каждого администратора ввести две учётные записи: непривилегированную – для повседневной работы (как «обычного» пользователя) и привилегированную – для выполнения задач администрирования ИТ-систем, обязать администраторов:

- **использовать привилегированную учётную запись только в случаях, когда без этого невозможно выполнить служебные задачи;**
- **перезагружать систему после применения на ней привилегированной учётной записи, что приведёт к очистке оперативной памяти и невозможности извлечь аутентификационные данные привилегированной учётной записи;**

- разработать и контролировать выполнение парольной политики (использовать менеджеры паролей, запретить хранение и передачу паролей в открытом виде, предусмотреть перезагрузку СВТ при смене паролей и т.д.)

Что делать?!!! (часть 3-я)

- ввести или актуализировать сегментацию (ограничить доверительные отношения между доменами, усилить их изоляцию (по возможности), использовать минимально необходимый набор портов и протоколов для сетевого обмена, минимизировать количество администраторов (доменов), техподдержке выдавать права локальных администраторов на только в зоне их ответственности и т.д.);
- периодически проверять и оценивать достаточность мер защиты электронной почты, организовать многоступенчатую фильтрацию входящего потока сообщений (как минимум, двумя защитными решениями);
- ввести двухфакторную аутентификацию для доступа к конфиденциальной информации и критически важным системам (например, контроллерам домена)

Что делать?!!! (часть 4-я)

- минимизировать или исключить права отладки(например, привилегию SeDebugPrivilege для локальных администраторах в Windows-системах);
- вывести сервисы, относящиеся к обеспечению информационной безопасности, в отдельный сетевой сегмент, передачу данных между этим сегментом и остальной сетью ограничить лишь минимально необходимым перечнем портов и протоколов для работы СЗИ и осуществления мониторинга с целью выявления инцидентов информационной безопасности;
- при необходимости удалённого доступа между сетевыми сегментами организовывать демилитаризованные зоны (DMZ), а сам удалённый доступ осуществлять через терминальные серверы

Что делать?!!! (часть 5-я)

➢ разработать и внедрить политику резервного копирования:

- **резервные копии должны храниться на отдельном сервере, не входящем в домен, откуда данные копии сохраняются;**
- **права на удаление и изменений резервных копий должны быть только у специально выделенной учетной записи, также не входящей в домен, откуда копии сохраняются;**
- **частота резервных копий таким образом должна исключать потерю критически важного объема информации;**
- **дублировать и обеспечить хранение 2-3 резервных копий для критически важных ресурсов, в частности, на автономном носителе информации;**
- **прописать процедуру проверок резервных копий;**
- **применять RAID-массивы для хранения резервных копий**

kaspersky

И да будет с нами целостность, доступность и конфиденциальность!!!

kaspersky

СПАСИБО за ВНИМАНИЕ!

Вопросы?

- **АО "Лаборатория Касперского"**
- **Москва, 125212**
- **Ленинградское шоссе, д.39А, стр.3**
- **+7 (495) 797-87-00**
- **www.kaspersky.ru**