ВЛАДИВОСТОК | ИНФОРМАЦИОННЫЙ ЦЕНТР | 22.06.2018

Трансформация рынка ИБ.
Современным вызовам – современные решения.

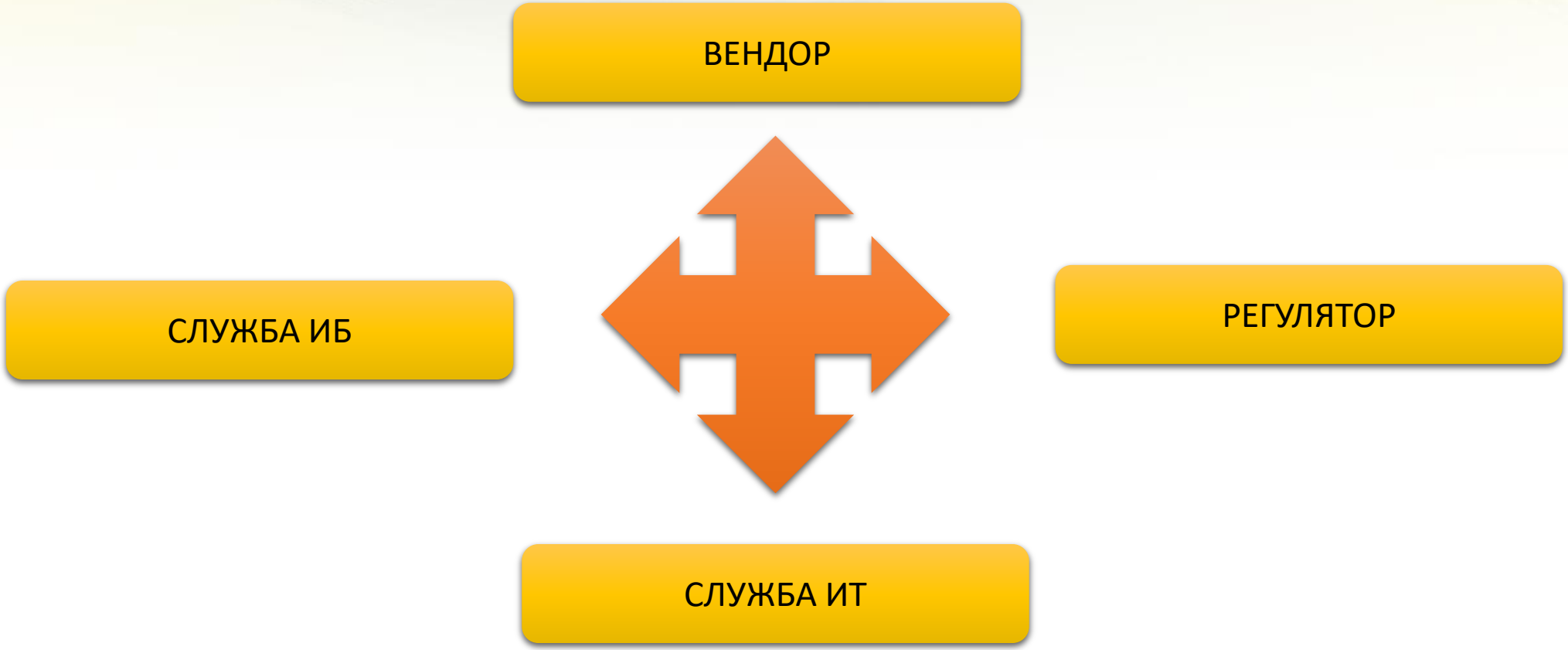
Лопатин Роман
Заместитель руководителя отдела продаж

ВОПРОС НА ЗАСЫПКУ

Яйцо или курица?

Информационная безопасность как парадигма не может проецироваться исключительно и только на одну составляющую информационных технологий. Обеспечить защиту данных нельзя, не обеспечив защиту самой инфраструктуры. Обеспечить защиту прикладного ПО нельзя без мер по защите ОС и аппаратных компонентов.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



КОД БЕЗОПАСНОСТИ

ИННОВАЦИОННОСТЬ ИЛИ КОНСЕРВАТИЗМ?

- Выполнение требований регуляторов
- Понимание ответственности за сохранность данных
- Выполнение отраслевых стандартов по ИБ
- Иметь задел для развития инфраструктуры и СЗИ

- Легко
- Быстро
- Доступно
- Бесперебойно

COMPLIANSE OR QUALITY?

- СЗИ должны работать
- Гибкость разработки
- Скорость разработки
- Учитывание WORLD BEST PRACTICE

- СЗИ должны работать в рамках наших требований
- Сертификация как подтверждение работоспособности
- Мы успеваем за изменениями ИТ/ИБ ландшафта
- Жёсткая привязка к отечественной разработке

РЕГУЛЯТОРЫ

Количество регуляторов увеличивается
Ответственность усиливается
Создаются новые ГИС и АИС
Происходит автоматизация всевозможных процессов, как для юридических лиц, так и для физических лиц.

ДА! ЭТО УДОБНО!

НЕТ! ЭТО НЕБЕЗОПАСНО!

РОСКОМНАДЗОР

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ

БАНК РОССИИ

Минкомсвязь России

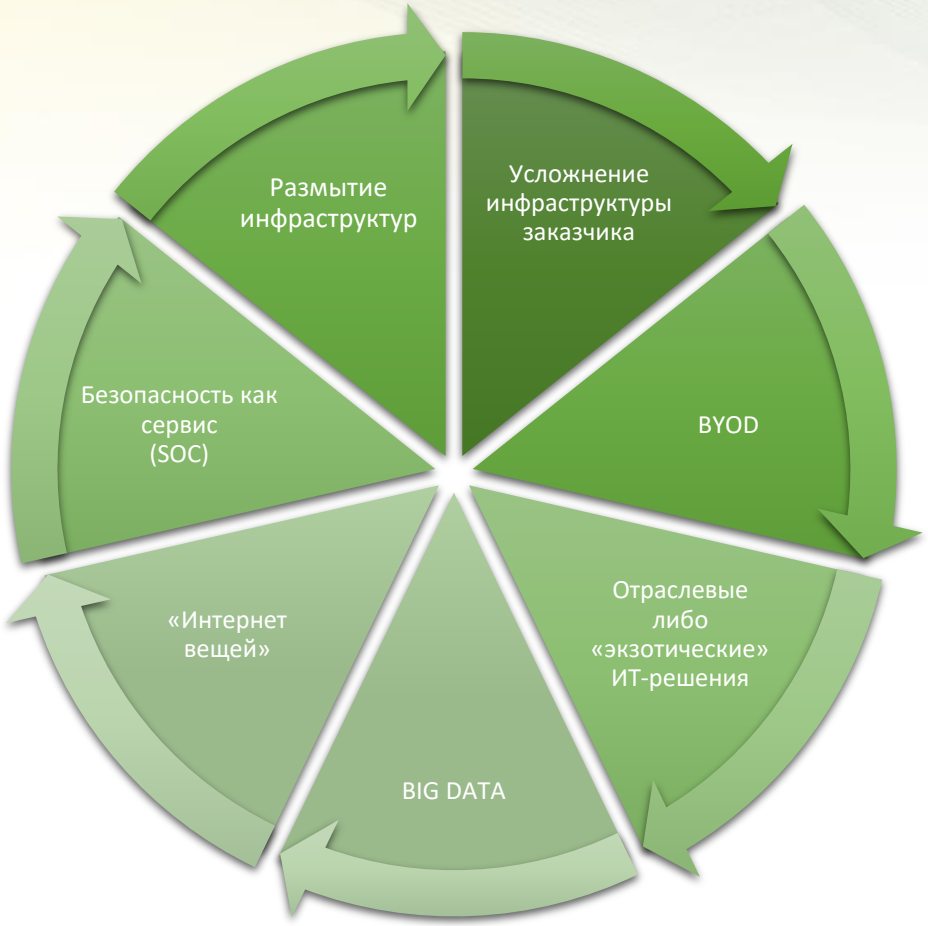
Министерство обороны Российской Федерации

НО ВСЕ СХОДЯТСЯ В ОДНОМ...

При этом все участники рынка прекрасно понимают, что любые активы компании, организации, органа власти должны быть защищены.

- ✓ Вне зависимости от того, в рамках какой инфраструктуры они крутятся…
- ✓ Вне зависимости от наличия бюджетов, либо их отсутствия…
- ✓ Вне зависимости от качества и количества эксплуатируемых СЗИ/СКЗИ…
- ✓ Вне зависимости от зрелости технологий защиты и её актуальности на сегодняшний день…

ОБ ЭТОМ И ПОГОВОРИМ



Развитие ИТ-Технологий порождает новые тренды. Они прямо или косвенно проходят в нашу жизнь, быт, рабочие процессы.

В результате чего происходит изменение ландшафта самой инфраструктуры, методов обработки данных, их хранения, передачи.

Соответственно и взгляд на защищенность всей отрасли также трансформируется.

Конфиденциальность, целостность, доступность. Всё стало гораздо сложнее.

ПРОПАСТЬ И МЫ...

МЫ СЛИШКОМ ДАЛЕКО УШЛИ ОТ РЕАЛИЙ…

- ✓ Современные технологии и их применение на практике ушли вперед
- ✓ Тренды в ИТ/ИБ переросли в гонку вооружений
- ✓ Размытие периметра ЛВС произошло – революция свершилась! О чём очень сожалеют безопасники…
- ✓ Погоню за требуемыми компетенциями выдержат не все…
- ✓ Отсюда простой и очень очевидный вывод – трансформация как рынка ИБ, так и всех его участников будет здесь и сейчас. Выживут не все…

КОД БЕЗОПАСНОСТИ

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

ЦИФРОВИЗАЦИЯ

Цифровая трансформация – использование современных технологий для кардинального повышения производительности и ценности предприятий – на сегодня является горячей темой для компаний по всему миру.

В условиях цифровизации технологии преобразуют практически все коммерческие и производственные процессы, вынуждая компании переходить на автоматизированную цифровую платформу на основе данных и искусственного интеллекта.

WEB-ТЕХНОЛОГИИ

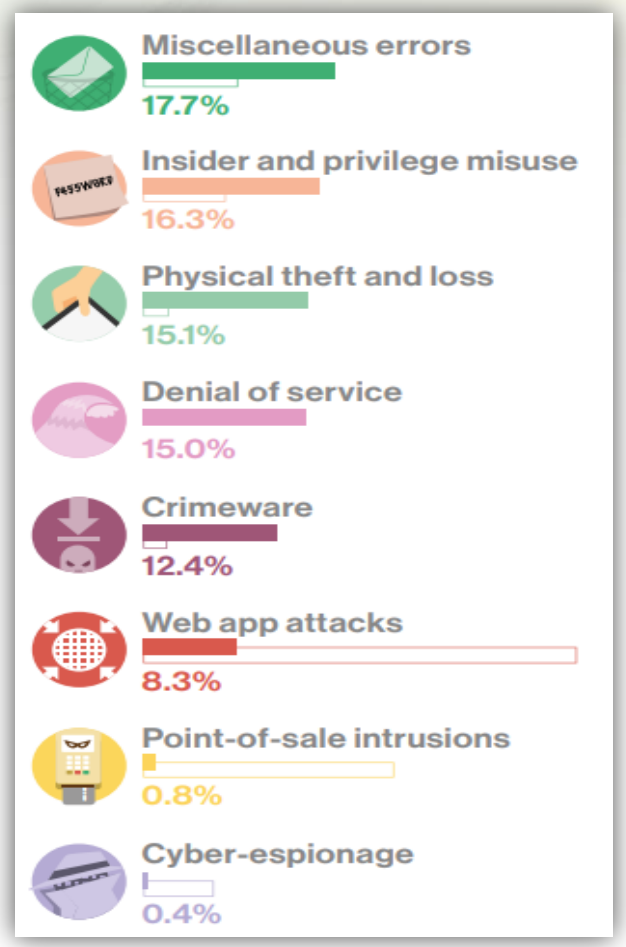
WEB

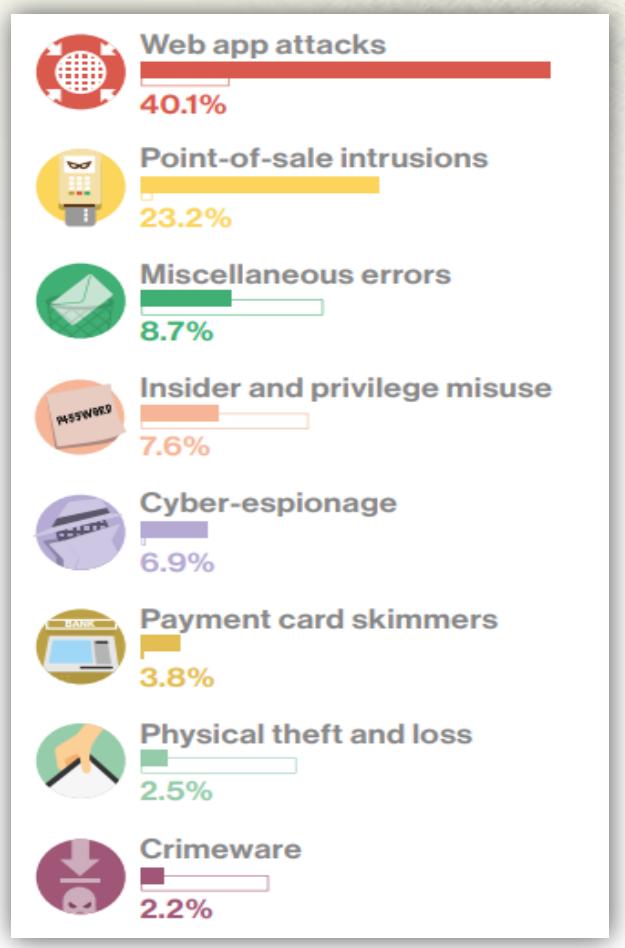
Веб-приложение — клиент-серверное приложение, в котором клиент взаимодействует с сервером при помощи браузера, а за сервер отвечает — веб-сервер.

Логика веб-приложения распределена между сервером и клиентом, хранение данных осуществляется, преимущественно, на сервере, обмен информацией происходит по сети.

Одним из преимуществ такого подхода является тот факт, что клиенты не зависят от конкретной операционной системы пользователя, поэтому веб-приложения являются межплатформенными службами.

verizon





МОБИЛЬНЫЕ УСТРОЙСТВА

BYOD

BYOD (bring your own device, принеси собственное устройство) - термин, описывающий ситуацию, когда сотрудник организации вместо корпоративного компьютера использует для работы собственное устройство, будь то его личный ноутбук, планшет или, в предельных случаях, даже смартфон.

BYOD - не финал, а лишь концепция, переходная форма между классическим неподвижным компьютером на рабочем столе и неким новым подходом к организации работы с целью обеспечить максимальный комфорт и продуктивность сотрудника, дав ему возможность работать там, тогда и таким образом, как он хочет.

ОБЛАЧНЫЕ СЕРВИСЫ

CLOUD

Облачные сервисы — это сервисы, работающие на облачных хранилищах. То есть, их не нужно устанавливать на компьютер и получать доступ с любой точки выхода. В онлайн (облачных) хранилищах данные хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной.

В отличие от модели хранения данных на собственных выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту, в общем случае, не видна.

КОД БЕЗОПАСНОСТИ

БИОМЕТРИЧЕСКАЯ ПЛАТФОРМА

БИОМЕТРИЯ

Биометрия предполагает систему распознавания людей по одной или более физическим или поведенческим чертам.

В области информационных технологий биометрические данные используются в качестве формы управления идентификаторами доступа и контроля доступа.

ЦЕНТРЫ МОНИТОРИНГА

Безопасность как сервис (SOC & CERT)

SOC — Security Operations Center, или Центр оперативного управления, основными задачами которого являются консолидация событий из множества источников, проведение определенной аналитики и оповещение уполномоченных сотрудников об инцидентах информационной безопасности или иных происшествиях. На основе полученных данных сотрудники центра проводят расследование, принимают меры, чтобы исключить возможность повторения события, минимизируют потери.

CERT (Computer Emergency Response Team) — это МЧС в цифровом мире, в число основных задач которого входят сбор информации о событиях ИБ, их классификация и нейтрализация. Примерами таких CERT являются соответствующие структуры при Управлении «К» МВД России и ЦИБ ФСБ России, включая созданный при участии ФСБ России сайт gov-cert.ru

КОД БЕЗОПАСНОСТИ

ПОПРОБОВАТЬ ПРЕВЗОЙТИ или ВЫЗОВ ПРИНЯТ

- Межсетевое экранирование
- Криптография – защита каналов связи
- Web Application Firewall
- Проактивная защита периметра (IPS/IDS)
- Криптография – шифрование SSL.
- Next Generation Firewall/UTM

- Каналообразующее оборудование
- Серверные компоненты
- Автоматизированные рабочие станции
- Терминальные и тонкие клиенты

FORTINET

CISCO

JUNIPER NETWORKS

f5

HUAWEI

Lenovo

D-Link

DELL

hp

Check Point SOFTWARE TECHNOLOGIES LTD.

paloalto networks

ARBOR NETWORKS

ПОПРОБОВАТЬ ПРЕВЗОЙТИ или ВЫЗОВ ПРИНЯТ

- Прикладное ПО
- Антивирусная защита
- Операционные системы
- СУБД
- Резервное копирование
- Платформы виртуализации
- Офисные приложения
- ERP-системы
- Веб-приложения

VEEAM

SAP

AUTODESK.

vmware

Adobe

ORACLE

McAfee

Symantec

ПРОПРИЕТАРНЫЕ ОС

Microsoft выпустила обновление Windows и убила компьютеры

439 82 50 Добавить в «Мою Ленту»

Фото: Matthias Balk / DPA / Globallookpress.com

Корпорация Microsoft приоста
для Windows, которое закрыва
причиной полного отключени
вторник, 9 января, сообщает The Verge.

В Windows обнаружена худшая за последнее время критическая уязвимость (Обновлено)

Теги: Windows, Microsoft, уязвимость

Уязвимость позволяет осуществлять самовоспроизводящиеся атаки.

Два ИБ-эксперта Google обнаружили критическую уязвимос
код. Рабо
Силванович (Natalie Silvanovich) и Тэвис
проблему, как «худшую на их памяти уяз
выполнить код».

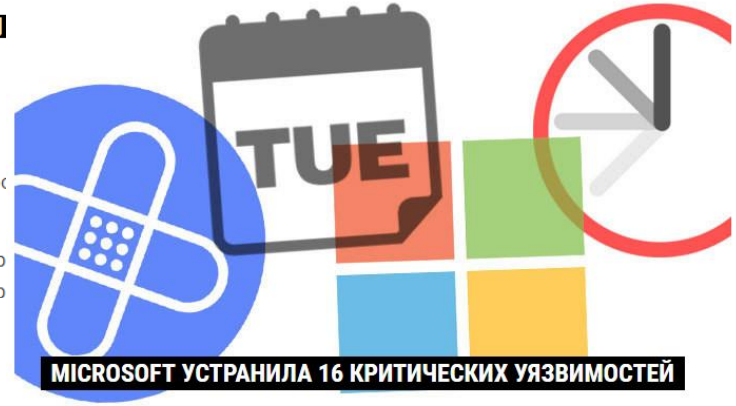
В Microsoft объяснили, как защититься от новых уязвимост

12.01.2018, 13:05 Текст: Виктория Чернышева

В 4 1

На официальном сайте Microsoft появилось официальное заявление, в котор
рассказывается о новых уязвимостях и о том, как от них защититься.

Как уточнил исполнительный вице-президент группы Windows и Devices Терр
Майерсон, риску подвержены пользователи смартфонов и ПК, а также сервер



Текст Tom Spring 11 января 2018 , 15:53

Публикация уязвимостей Meltdown и Spectre уже сделала январь весьма жарким месяцем для специалистов Microsoft по подготовке исправлений. Традиционный «вторник патчей» корпорация отметила выпуском заплат для десятков других брешей, в том числе в Microsoft Edge, Windows, Office, ASP.NET и версии Office для

Microsoft выпустила экстренный патч для критической RCE-уязвимости в Windows

Мария Нефёдова , 10.05.2017 3 мин на чтение 0 2 30711

ПО И ОБОРУДОВАНИЕ

В компоненте SAP NetWeaver обнаружены опасные уязвимости

Уязвимости могут привести к раскрытию информации, повышения привилегий и полной компрометации системы SAP CRM.

Спустя четыре года SAP исправила уязвимость в SAP NetWeaver AS JAVA P4

Уязвимость обхода аутентификации в P4 предоставляет хакерам возможность раскрыть важные данные.

В продуктах SAP исправлены 26 уязвимостей

Наиболее опасные уязвимости позволяют скомпрометировать систему и осуществить DoS-атаку.

SAP исправила опасные уязвимости в своих продуктах

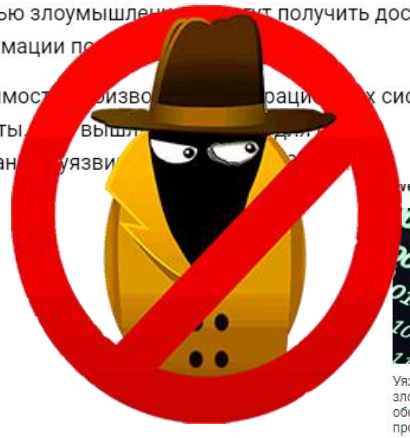
Систему SAP POS удалось взломать с помощью ноутбука и карманного Raspberry PI за $25

3 января пресса сообщила о серьёзной уязвимости процессоров Intel на уровне архитектуры. С её помощью злоумышленн получить доступ к ядру процессора и личной информации по

Вскоре после обнаружения уязвимост изво раци х систем начали спешно выпускать апдейты. вышл Windows 10. Apple частично устран уязви

Текст Julia Glazova 7 апреля 2018 , 02:39

В Интернете зафиксирован всплеск активности бота, эксплуатирующего новую брешь на устройствах под Cisco IOS.



Атака на коммутаторы Cisco в работе ряда

200 тыс. сетевых со по всему миру.

Уязвимость в коммутаторах Cisco используется для атак на объекты КИ по всему миру

Некоторые из атак были проведены группировкой, известной как Dragonfly, Crouching Yeti и Energetic Bear.

Cisco опубликовала годовой отчет по информационной безопасности

Для защиты от киберугроз специалисты рекомендуют внедрять новые технологии безопасности, включающие машинное обучение и способности искусственного интеллекта.

бэкдор из своей системы IOS XE

XE 16.x скрытой учетной анию с именем sco» и статическим

В решении Cisco Elastic Services Controller обнаружена опасная уязвимость

Злоумышленник может авторизоваться в учетной записи администратора с пустым полем пароля.

Cisco устранила критическую уязвимость в своих межсетевых экранах

Проблема позволяет удаленно выполнить код и получить контроль над устройством.

ила ряд язвимостей в

Уязвимости позволяют удаленному злоумышленнику добиться отказа в обслуживании и выполнить произвольный код.

Как обезопасить умный автомобиль? Мнение экспертов из «ИнЧип» и Cisco

Хакерам ничего не стоит дистанционно взломать компьютерную систему смарткара.

Cisco устранила опасные уязвимости в ПО IOS

В общей сложности Cisco исправила 13 уязвимостей.

КОД БЕЗОПАСНОСТИ

ПРИЧЕМ ЗДЕСЬ МЫ

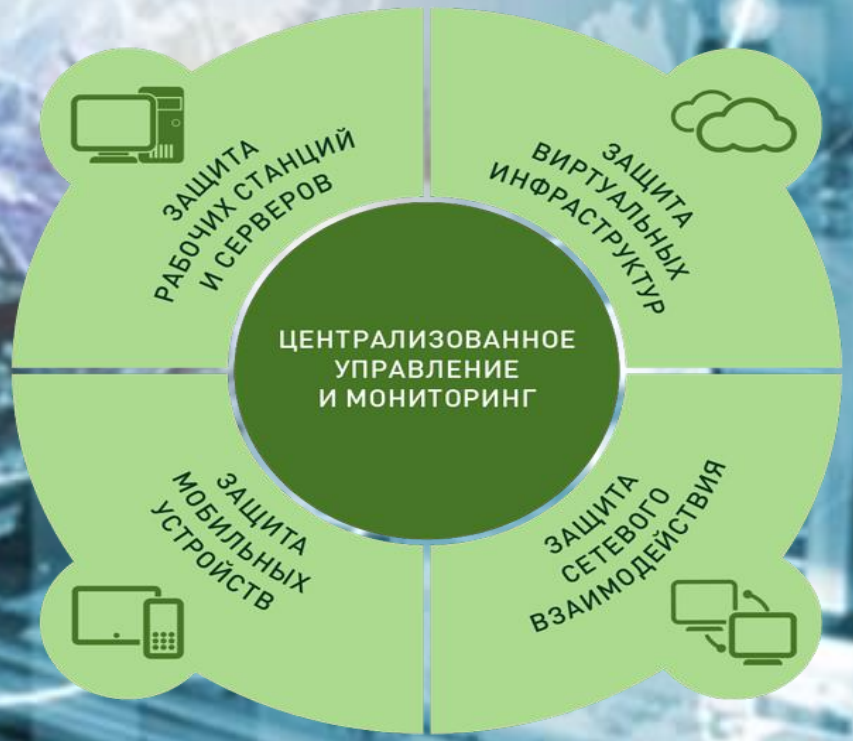
Ведущий российский разработчик средств защиты информации.

Самый широкий портфель решений по ИБ.

3 центра разработки – Москва, Санкт-Петербург, Пенза. Более 300 разработчиков.

Полный цикл работ.
Проектирование, внедрение, сопровождение.

Более 70-ти сертификатов ФСТЭК, ФСБ, МО на всю продуктовую линейку.



КОД БЕЗОПАСНОСТИ

К ЧЕМУ МЫ ИДЕМ?

ПАК «СОБОЛЬ» 4.0

ДОВЕРЕННАЯ СРЕДА

SECRET NET STUDIO

ПАК «СОБОЛЬ» 4.0

- ✓ Поддержка UEFI-Биоса
- ✓ Контролирует целостность как «железа», так и загрузки легитимной ОС
- ✓ Проводит двухфакторную аутентификацию
- ✓ Регистрирует попытки доступа к АРМ

ДОВЕРЕННАЯ СРЕДА

- ✓ Контролирует системные файлы и процессы на АРМ
- ✓ Блокирует все возможные поползновения на целостность и работоспособность любых СЗИ
- ✓ Блокирует возможность подмены системных .dll и драйверов

SECRET NET STUDIO

- ✓ Замкнутая программная среда
- ✓ Контроль действий учётных записей
- ✓ Разграничение доступа и контроль привелигированных пользователей
- ✓ Централизованное обновление всеми защитными компонентами

К ЧЕМУ МЫ ИДЕМ?

vGate 4

vGate for CLOUD

vGate 4 FW

- ✓ Контроль привилегированных пользователей
- ✓ Усиленное управление доступом в среде виртуализации
- ✓ Контроль целостности ВМ
- ✓ Соответствие требованиям (compliance)
- ✓ Централизованное управление и мониторинг
- ✓ Сетевая защита (Межсетевой экран - Централизованное управление правилами фильтрации во всей виртуальной инфраструктуре)
- ✓ Обнаружение инцидентов (SIEM – мониторинг безопасности . Сбор, нормализация, фильтрация, корреляция событий с ESX-хостов, модулей управления и средств защиты виртуальной среды).

КОД БЕЗОПАСНОСТИ

К ЧЕМУ МЫ ИДЕМ?

Континент 4

Континент TLS + WAF

Криптоакселерация

- ✓ Активно-активный кластер КШ с балансировкой нагрузки, масштабируемость
- ✓ Открытое распределение ключей (PKI)
- ✓ Кластеризация ЦУС
- ✓ Иерархическое управление ЦУС
- ✓ Система IPS в КШ
- ✓ DPI – (deep packet inspection)
- ✓ URL фильтрация (black листы Роскомнадзора)
- ✓ Агрегация портов
- ✓ Поддержка GREтоннелей
- ✓ Крипто-акселератор FPGA – модуль расширения для IPC-3000F, VPN 40Гбит full duplex
- ✓ Интеграция базы пользователей с MS AD
- ✓ Web Application Firewall

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Роман Лопатин

r.lopatin@securitycode.ru
+7 (495) 982 30 20 (*491)
+7 (926) 567 39 86