Перевод: английский - русский - www.onlinedoctranslator.com

BeyondTrust

2022 CYBERSECURITY SURVIVAL GUIDE

Recalibrate your Security for Today's Threats

BeyondTrust

ОГЛАВЛЕНИЕ

Резюме: Состояние кибербезопасности 3

Путь наименьшего сопротивления меняется 5
Ускоренная цифровая трансформация 5
Мультиоблачный мир с мультиоблачными проблемами 7
роста небезопасного удаленного доступа 8
Рост уязвимостей повсюду 11
Взрыв неуправляемых привилегированных удостоверений, доступа 12
и сессий. Взаимосвязь всего 14
Изменение угрозы физической безопасности 16

Векторы угроз набирают обороты 17
Число фишинговых атак растет, 17
количество бесфайловых атак растет, 18
программы-вымогатели побеждают 20

Как склонить чашу весов в сторону киберзлоумышленников 22
Стратегия выживания 1. Защита привилегированных учетных 25
данных. Стратегия выживания 2. Безопасный удаленный доступ. 30
Стратегия выживания 3. Примените управление привилегиями конечных точек. Стратегия выживания 33
4. Примените усиление защиты и управление уязвимостями. Стратегия выживания 5. Предотвратите 37
вмешательство в мобильные и удаленные конечные точки. Стратегия выживания 6. Обеспечьте 39
безопасность и расширите возможности службы поддержки. 42
Стратегия выживания 7: тщательно проводите тестирование на проникновение удаленных работников 44

Перекалибруйте свою безопасность с помощью BeyondTrust 49

Дополнительные ресурсы 52

УПРАВЛЯЮЩЕЕ РЕЗЮМЕ

Штат

Информационная безопасность

Ожидается, что многие изменения на рабочих местах, ускоренные пандемией, сохранятся, и более устойчивая гибридная рабочая среда укоренится.

«Новая нормальность» уже здесь.

The Wall Street Journal назвал гибридное рабочее место «кошмаром кибербезопасности» и охарактеризовал его как «мечту хакера — постоянно меняющееся сочетание офисных и удаленных работников, устройств, которые входят и выходят из сетей компании, а сотрудники службы безопасности истощены». » The Wall Street Journal также вкратце описал, как организации получают контроль над этой средой — с сильной безопасностью, ориентированной на идентификацию, и нулевым доверием.[1]

ЭТО РУКОВОДСТВО ВКЛЮЧАЕТ:

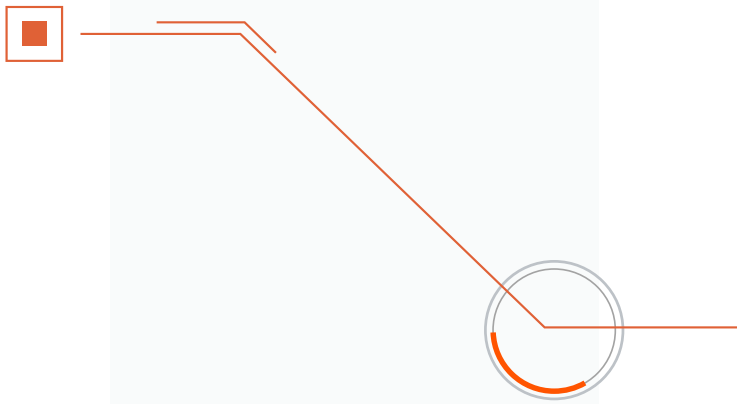
1. Данные, подтвержденные исследованиями, и анекдоты, иллюстрирующие, как меняется поверхность атаки.
2. Анализ того, как смещается путь наименьшего сопротивления субъекта угрозы
3. Анализ нескольких потрясших мир нарушений за последний год и того, как их можно было устранить в несколько этапов.
4. Советы по выживанию, которые помогут вам адаптироваться, устранить бреши в безопасности и снизить риски — и при этом получить выгоду для бизнеса от возможностей, предоставляемых новой реальностью.

Читайте дальше, чтобы понять изменение ландшафта угроз и стратегии безопасности и технологии, которые вы можете разместить на месте, чтобы смягчить риски, позиционируя вашей организации, чтобы безопасно воспользоваться преимуществами цифровых технологий трансформация (DX) и удаленная работа.

1- Рандл, Джеймс. (2021, 8 июня). Почему гибридное рабочее место — это кошмар кибербезопасности. Журнал "Уолл Стрит.

Что

«Новая нормальность?»



Защита данных является движущейся целью в эпоху работы из любого места (WFA). По мере того, как путь наименьшего сопротивления (POLR) злоумышленника к корпоративным данным и активам меняется, должны меняться и приоритеты управления ИТ-рисками.Антивирусное программное обеспечение (AV) пропускает 60% атак , а многие устройства IoT (Интернета вещей) и OT (технологии эксплуатации) не могут даже установить AV. Брандмауэры часто обходят или не имеют смысла в распределенных вычислительных средах, особенно в многооблачном мире.

Многие организации приобрели страховку киберответственности, чтобы защититься от финансовых затрат, связанных с кибератаками. Однако стремительные темпы и расширение масштабов киберугроз и атак с использованием программ-вымогателей побуждают компании киберстрахования резко увеличивать свои страховые взносы, требовать от своих клиентов определенных мер безопасности и подтверждения зрелости безопасности и даже отказываться от покрытия для организаций с высоким уровнем риска и определенных вертикальных рынков. . Некоторые поставщики киберстрахования вообще уходят из отрасли, в результате чего на рынке не хватает поставщиков, готовых подписать полисы.

Мы явно вступили в эпоху «предполагаемого нарушения» и «нулевого доверия». Поэтому нам необходимо не только переосмыслить безопасность, но и перекалибровать ее с учетом изменений в технологиях, которые происходят вокруг нас.

Путь наименьшего сопротивления меняется

Давайте рассмотрим еще несколько ключевых тенденций, которые формируют современную среду угроз.

Ускоренная цифровая трансформация

СогласноИсследование McKinsey , организации отреагировали на пандемию COVID-19, ускорив оцифровку взаимодействия с клиентами и цепочками поставок, а также своих внутренних операций на 3-4 года. McKinsey также обнаружила, что доля цифровых или цифровых продуктов в портфеле организаций увеличилась на целых 7 лет!

> «Внедрение цифровых технологий квантовый скачок как в организационный и отраслевой уровни. Наряду с многолетним ускорение цифровых технологий, кризис привел к кардинальным изменениям в мышлении руководителей о роли технологий в бизнесе».
>
> **- Исследование McKinsey & Co.**

Тем не менее, хотя цифровая трансформация пережила эволюционный квантовый скачок, изменилась и ситуация с киберугрозами. Проблема в том, что меры и стратегии кибербезопасности не претерпели соразмерного скачка в своей зрелости и, следовательно, отстают от современных угроз.

Угрозы безопасности, пробелы в соблюдении требований и уязвимости растут. Без сомнения, это играет ключевую роль в ошеломляющем масштабе и количестве инцидентов и нарушений кибербезопасности с конца 2020 года.

SolarWinds, Verkada, Colonial Pipeline, JBS, Kaseya и продолжающаяся волна разрушительных атак программ-вымогателей — это недавние примеры угроз, ставящих под угрозу цепочки поставок и влияющих на повседневную жизнь многих миллионов людей.

Хотя быстрое ускорение цифровой трансформации помогло организациям внедрять инновации, повысить эффективность и обеспечить более удаленную работу, оно также склонило чашу весов в бесконечной гонке кибервооружений в пользу преступников.

Сегодня удаленные работники часто работают с использованием незащищенного Wi-Fi или личных устройств. Многие пользователи самостоятельно устанавливали различные приложения, часто называемые «теневыми ИТ», чтобы продуктивно работать дома или в дороге. Технологии удаленного доступа, такие как VPN (виртуальная частная сеть) и RDP (протокол удаленного рабочего стола), обычно расширяются для случаев использования, выходящих далеко за рамки безопасного.

Злоумышленникам стало проще, чем когда-либо, найти эти бреши в безопасности и доставить вредоносные полезные данные, включая программы-вымогатели.

94%

компаний испытал влияние на бизнес кибератака или компромисс по поводу последний год[2]

Рекордный результат

количество киберпреступность жалобы в ФБР в 2020 году[3]

69%

Увеличение по сравнению с прошлым годом в жалобах ФБР[3]

2. Рост популярности руководителей служб безопасности, ориентированных на бизнес.
Forrester Consulting (по заказу Tenable), август 2020 г.

3- Отчет о преступности в Интернете (ICR) за 2020 г., ФБР, март 2021 г.

Многооблачный мир,

с задачами мультиоблачной среды

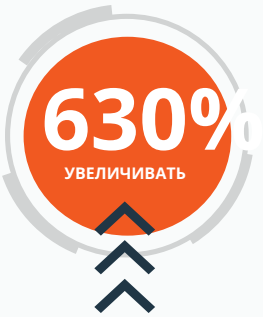
Поверхность облачных рисков значительно расширилась в ходе недавнего ускоренного периода цифровой трансформации. Сегодня большинство организаций находятся не просто в «облаке» — они находятся во многих облаках (PaaS, IaaS), и их конечные пользователи потребляют все больше приложений SaaS, большая часть которых происходит в виде теневых ИТ.

ИТ-команды изо всех сил пытаются контролировать безопасность в сложной среде управления несколькими облаками, каждое из которых имеет свои собственные модели общей ответственности и собственные наборы инструментов.

Кроме того, большинство компаний не являются полностью облачными — они работают по гибридной модели, включающей локальную инфраструктуру, часто основанную на устаревших технологиях.

Злоумышленники могут использовать мощные бесплатные инструменты, такие как Shodan, чтобы сосредоточиться на незащищенных облачных ресурсах и учетных записях. Плоскости управления, которые управляют всей облачной инфраструктурой, часто неадекватно заблокированы или подключены к Интернету, что делает их уязвимыми для атак методом перебора и других эксплойтов.

Отсутствие надлежащего контроля также приводит к неправильным конфигурациям, которые могут привести к сбоям в работе или раскрытию сегментов данных.



в угрожающих действиях

велось в облаке

услуги внешних

актеры начала 2020 года[4]

4. Отчет McAfee о внедрении облачных технологий и рисках, 2021 г.

Рост небезопасного удаленного доступа

За последнее десятилетие большинство нарушений ИТ-безопасности совершались удаленно. Хотя удаленный доступ обеспечивает необходимое удобство для сотрудников, подрядчиков, поставщиков и аудиторов, он также позволяет злоумышленникам обойти все физические меры контроля и потенциально получить прямой доступ к ресурсам и данным. Таким образом, удаленный доступ оказался путем наименьшего сопротивления личностям, доступу и данным, которые ищут субъекты угроз.

Неподготовленные к наплыву удаленных сотрудников, ИТ-команды поспешно разработали новые пути удаленного доступа для поддержания производительности, одновременно соблюдая директивы по социальному дистанцированию.

Сегодня организации являются

регулярно растягивающие инструменты, такие как

VPN и RDP выходят далеко за рамки своих

безопасные и правильные варианты использования.

Например, VPN никогда не следует использовать на личных устройствах сотрудников или поставщиков, поскольку они не могут обеспечить детальный контроль доступа, необходимый для привилегированных сеансов. Эта бессистемная инфраструктура удаленного доступа, которая первоначально предполагалась как краткосрочное решение, сохраняется во многих организациях и создает чрезвычайно простой вектор атаки, который киберпреступники могут использовать и закрепиться на начальном этапе.

Порты RDP с выходом в Интернет увеличены на 50 %. в первые месяцы пандемии, чтобы срочно поддержать инициативы по работе на дому (WFH). RDP, доступный в общедоступный Интернет, является хорошо известным табу безопасности, но это происходит регулярно, и часто с наиболее конфиденциальными ресурсами. Неправильное использование и недостаточно защищенный протокол RDP сыграли огромную роль в том, что за последний год открылись широкие двери для программ-вымогателей, вредоносных программ, фишинга и других векторов атак.

В последние пару лет организации в значительной степени опирались на VPN для быстрого расширения удаленного доступа, однако это опасное несоответствие для многих случаев использования, например, для поставщиков, привилегированных пользователей/сессий и пользователей, работающих на BYOD.

Технология VPN была создана для обеспечения доступа и защиты данных, передаваемых за пределы традиционной сети компании, и ее следует рассматривать скорее как инструмент обеспечения бизнеса, чем как инструмент кибербезопасности.

Поскольку VPN обычно предоставляют открытый доступ к сети, они опасно предполагают надежность и бескомпромиссность всего в VPN. Это само по себе является серьезным нарушением безопасности, которое нарушает принципы нулевого доверия.

В конечном итоге ваша безопасность может быть такой же хорошей, как у внешней конечной точки или пользователя, которому вы разрешаете туннелировать в вашу среду.

> *RDP был замешан как один из самых распространенных методы нарушения сеть в тех случаях, когда мы были вызвали для расследования, вот почему выключение доступ к внешнему миру RDP является одним из наиболее эффективная защита и ИТ админ может взять.*
>
> Эндрю Брандт, главный исследователь SophosLabs

[Новости Sophos, июнь 2021 г.]

Отсутствие детального контроля и прозрачности сеансов туннелирования VPN — это лишь часть проблемы. Десятки уязвимостей VPN используются, что приводит к крупным нарушениям в бизнесе и правительстве.

Эту проблему усугубляет тот факт, что исправления для VPN-устройств и программного обеспечения часто забывают или игнорируют. Те компании, которым требуется доступ к VPN для сотрудников для выполнения своей работы, часто сталкиваются с противодействием окнам обслуживания исправлений VPN или даже с заменой старой технологии VPN.

Хакеры знают, что если они смогут взломать VPN, во многих случаях им больше не придется беспокоиться о традиционных средствах безопасности, таких как брандмауэры, — они получат полный доступ к сети компании.

Брандмауэры мало что могут сделать, чтобы заблокировать нежелательный трафик, когда вы открыто предоставляете доступ к сети через VPN. Кроме того, VPN сложно правильно настроить, и они часто неправильно настраиваются, создавая бреши, через которые злоумышленники могут получить доступ, особенно при попытке предоставить детальный доступ большому количеству пользователей.

Удаленные работники также создают множество дополнительных рисков, связанных с самим удаленным доступом, в том числе:

- Использование незащищенных домашних и общественных сетей Wi-Fi.
- Использование личных устройств (BYOD), которым не хватает адекватной защиты и других базовых средств защиты. Совместное использование
- устройств с другими членами семьи для работы, учебы и отдыха.

- Перемещение вперед и назад между несколькими местами, будь то дом, офис или другое пространство.

Рост уязвимостей повсюду

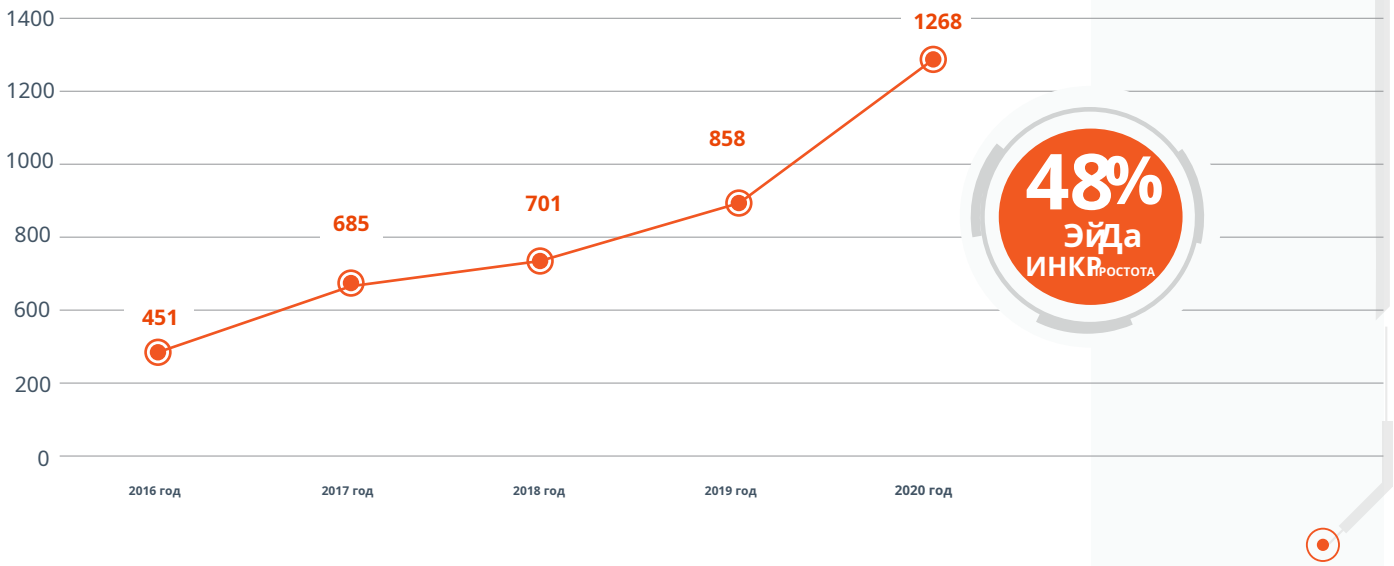
Тот факт, что злоумышленники используют известные уязвимости, не является чем-то новым — это одна из старейших истин ИТ-безопасности. Тем не менее, эта практика по-прежнему обеспечивает злоумышленникам высокий уровень успеха и является распространенным компонентом цепочек атак.

В конце 2020 годаФБР и CISA предупредили что субъекты, использующие сложные постоянные угрозы (APT), нацелены на правительственные сети, критическую инфраструктуру и избирательные организации с помощью кибератак с цепочками уязвимостей. Эти атаки объединяли устаревшие уязвимости, чтобы закрепиться и продолжить атаку.

Такие атаки можно легко предотвратить на нескольких этапах, просто установив исправления. Однако уязвимости нулевого дня можно (потенциально) устранить только с помощью других тактик (таких как управление привилегированным доступом, усиление защиты и т. д.) до тех пор, пока не будет доступен патч.

Последнее издание BeyondTrust'sежегодный отчет Microsoft об уязвимостях обнаружили, что общее количество опубликованных уязвимостей Microsoft достигло рекордного уровня в 2020 году, увеличившись на 48% по сравнению с предыдущим годом. Этот вывод еще раз подтверждает мнение о том, что уязвимости и поверхность атаки быстро расширяются, отчасти из-за «квантового скачка» в цифровой трансформации.

Опубликованные уязвимости Microsoft в 2020 году



Взрыв неуправляемых привилегированных удостоверений, доступа и сеансов

Еще один примечательный вывод из отчета Microsoft об уязвимостях за 2021 год заключался в том, что в 2020 году «Несанкционированное повышение привилегий» было самой распространенной уязвимостью Microsoft, составляющей 44% всех уязвимостей.

Повышение привилегий уязвимости утроились с 2019 по 2020 год.

Чем больше привилегий имеет часть программного обеспечения или приложения, пользователь, учетная запись или процесс, тем больше вероятность злоупотреблений, эксплойтов или ошибок. Сегодня многие уровни привилегий создаются в огромных масштабах благодаря цифровой трансформации, расширению облачных технологий, виртуализированным средам, Интернету вещей, периферийным вычислениям, теневым ИТ и т. д.

Привилегии человека и машины, которые долгое время были слабым местом в системе безопасности, становятся все сложнее обнаруживать и контролировать в этом обширном децентрализованном ИТ-ландшафте, поскольку они действительно могут находиться где угодно.

Наши клиенты говорят нам, что идентификаторы машин растет в два раза быстрее человеческих идентичностей.

Форрестер Волна™:

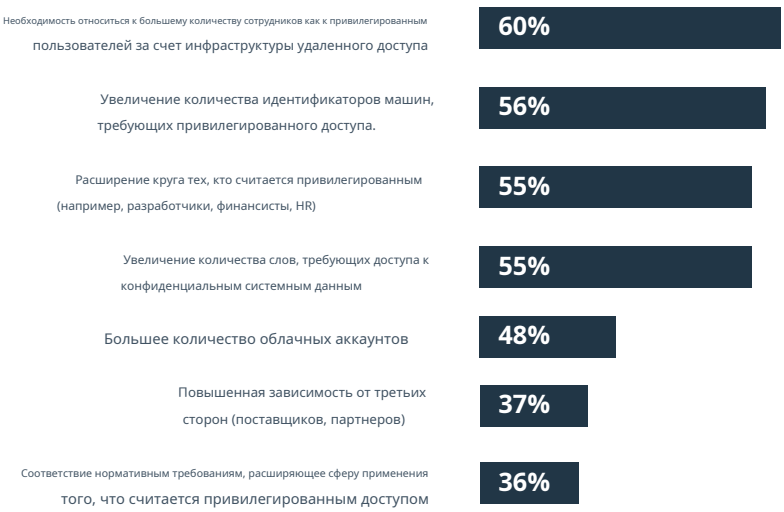
Привилегированная личность Менеджмент, 4 квартал 2020 г. Форрестер Исследования

В случае кибератаки разница между сдерживанием атаки и успехом и распространением атаки часто сводится к тому, способен ли злоумышленник добиться горизонтального движения.

Обычно для этого требуется привилегированная учетная запись или использование критической уязвимости. Доступ к привилегированной учетной записи также может облегчить злоумышленнику сканирование портов и использование встроенных системных инструментов для проведения разведки, очистки следов и достижения дальнейшего повышения привилегий.

В исследованииBeyondTrust по заказу Forrester Consulting Большинство опрошенных организаций прогнозируют увеличение числа привилегированных учетных записей и привилегированных сеансов в течение следующих двух лет. Этот рост во многом обусловлен аспектами цифровой трансформации.

Почему вы ожидаете, что количество привилегированных сеансов (человеческих или компьютерных) в вашей организации увеличится в ближайшие два года?



База:241 специалист по ИТ-безопасности и эксплуатации в Северной Америке, ЕС или Азиатско-Тихоокеанском регионе.

Источник:Азаказное исследование проведено Forrester Consulting по поручению BeyondTrust, июнь 2020 г.

Хрупкость цепочки поставок, критическая инфраструктура под угрозой и взаимосвязанность всего

За последние пять лет количество атак на цепочки поставок, которые ставят под угрозу надежное программное или аппаратное обеспечение и проникают в число новых жертв, растет, достигнув впечатляющего крещендо в 2021 году.

ЕщеGartner ожидает, что 45% организаций по всему миру к 2025 году подвергнутся атакам на свои цепочки поставок программного обеспечения, что в три раза больше, чем в 2021 году.

Компрометируя самое слабое звено — удаленного работника, подрядчика, недостаточно защищенную систему, пользователя с чрезмерными привилегиями, неконтролируемую идентификацию машины, незащищенные порты или уязвимость VPN — злоумышленник может проникнуть в организацию и поставить под угрозу программное обеспечение, используемое тысячами клиентов, как это произошло с Нарушения SolarWinds и Kaseya и многие другие.

Многое из того, что происходит называемая «новой нормой», не совсем новый – просто это более выражено.

Крайне разрушительный и широко звучащий цепочка поставок и критически важные нарушения инфраструктуры подчеркнули взаимосвязь и, следовательно, хрупкость из всего.

Еще одна проблема, имеющая далеко идущие последствия, заключается в том, что части OT и АСУ (систем промышленного управления) все чаще подключаются к Интернету и их легко обнаружить, что потенциально ставит под угрозу безопасность всей критически важной инфраструктуры, большая часть которой является устаревшей ИТ.

Отчет Claroty о рисках и уязвимостях АСУ ТП, выходящий два раза в год: второе полугодие 2020 г. обнаружили, что 70% выявленных недостатков в АСУ ТП можно использовать удаленно, что показывает, что эти системы, как правило, больше не полностью изолированы от внешних кибератак.

В 2021 году мир потрясли такие нападения, как попытка отравления воды на водоочистной станции во Флориде (Олдсмар) и прорыв колониального трубопровода, в результате которого 45% топлива, поставляемого в регион восточного побережья США, были полностью отключены на несколько месяцев, что привело к масштабные сбои и рост цен на топливо.

OT-системы особенно сложно исправлять из-за устаревшего характера технологии, сложности окружающей среды, а также проблем и затрат, связанных с потенциальным сбоем. Поэтому для этих систем особенно важно тщательно применять правильную сегментацию, управление привилегированным доступом, управление паролями и другие передовые методы усиления защиты и безопасности.

Кроме того, OT больше не относится только к таким вещам, как коммунальные услуги и заводы. Интернет вещей и распространение «умных» вещей означают, что отрасли и предприятия, в том числе компании по управлению недвижимостью, которым может потребоваться управление «умными» зданиями, должны учитывать уязвимости и риски безопасности так, как они этого не делали раньше.

В 2020 году 54% всех Драгош обязательства по оказанию услуг включил вывод о общие учетные данные в OT системы и 100% Реагирование на инцидент в Драгосе (IR) вовлеченные обязательства общие учетные данные, которые эксплуатировались для бокового движение. Далее, 88% обязательств по оказанию услуг также включен вывод про неадекватную сеть сегментация.[5]

5- Обзор кибербезопасности ICS за 2020 год. Драгош. февраль 2021 г.

Изменение угрозы физической безопасности

Наконец, организации сталкиваются с повышенной угрозой физической безопасности, причем не для корпоративных офисов и серверных помещений, а для удаленных и мобильных конечных точек, многие из которых получают доступ к конфиденциальным данным и хранят их, а также регулярно выполняют привилегированные действия.

Этими устройствами (ноутбуками, смартфонами, планшетами и т. д.) могут быть:

- В домохозяйствах, где проживают соседи по комнате или члены семьи. В
- общественных местах с высоким уровнем воровства, нацеленных на мобильные телефоны, планшеты и ноутбуки.
- Электронная компрометация, например, путем взлома SIM-карты, создание физического электронного клона.

Хотя риск кражи и BYOD мобильных устройств (смартфонов, ноутбуков и т. д.) существует и растет уже более десяти лет, сегодня его масштабы во много раз выше. Злоумышленник теперь может предположить, что корпоративное устройство сотрудника, скорее всего, находится у него дома.

Если злоумышленник-инсайдер получил доступ к ноутбуку или устройство было украдено из чьего-то дома, ничто не мешает злоумышленнику разобрать его и удалить важные компоненты, такие как жесткий диск, или, возможно, даже добавить вредоносное оборудование для наблюдения. Когда сотрудник находится дома или в общественном месте, обычно не существует современных средств физической защиты для предотвращения кражи или манипуляций с устройствами такого типа.

Поверхность атаки значительно увеличивается

Больше уязвимостей

Больше удаленного доступа

Больше привилегий

Больше теневых ИТ

Подробнее BYOD / BYOT

Больше облаков

Больше цифровых технологий

Трансформация

Больше идентичностей (человек, машина и т. д.)

Больше связей из всего

Векторы угроз

Нагрев

Значительно увеличивающаяся поверхность атак создает благодатную среду для разнообразия субъектов угроз и видов атак.

В этом разделе мы выделим три наиболее заметно растущих тенденции угроз: фишинг, бесфайловые атаки и программы-вымогатели.

Фишинговые атаки растут

«В результате значительного расширения цифрового поверхность атаки, количество фишинговых атак выросло на 600%, включая фишинговые атаки на тему Covid-19 нацелен на работников, совмещающих личное и рабочее устройства через незащищенные сети Wi-Fi. Большинство из них связаны с удаленной работой. нарушения произошли из-за отсутствия видимости со стороны администраторы над политиками доступа сотрудников и уязвимые конечные точки».

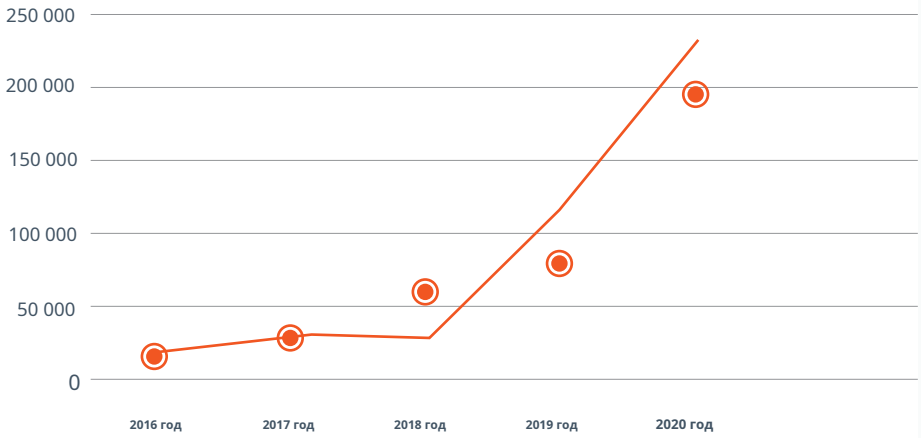
Чак Брукс,

Эксперт по кибербезопасности, преподаватель Джорджтаунского факультета. ***Отчет BeyondTrust об уязвимостях Microsoft за 2021 год***

Фишинговые атаки стремительно набирают обороты, при этом злоумышленники идут ва-банк с этими эксплойтами социальной инженерии, направленными против множества уязвимостей и брешей в безопасности, которые были созданы огромным количеством удаленных сотрудников.

Фишинг, социальная инженерия и компрометация диска были наиболее распространенными методами первоначального доступа, наблюдаемыми BeyondTrust Labs с мая 2020 г. по май 2021 г. Фишинг в течение многих лет оставался основным вектором первоначальной компрометации среды, например, с помощью вредоносной ссылки или вложения, а также для сбора информации, которая впоследствии может быть использована для использования обнаруженной уязвимости.

Количество жалоб на фишинговые преступления, поступивших в Центр рассмотрения жалоб на интернет-преступления ФБР



Включает жалобы на вишинг, смишинг и фарминг. **Источник:** Центр жалоб на интернет-преступления

Ожидание получение законного коммуникации по электронной почте — часто от неизвестного или непредвиденные источники — облегчает задачу нападающий для достижения высокого процент успеха, особенно если они смогут адаптировать атака на основе имеющихся исследования или утечка данных на своей цели.

Бесфайловые атаки растут

В 2020 году количество атак без файлов, часто называемых атаками с использованием земли (LotL) или атаками с нулевым следом, резко возросло на 888%. Эти хитрые угрозы часто используют против себя собственные законные инструменты организации-жертвы (PowerShell, Wscript и т. д.).

Бесфайловые вредоносные программы являются ключом к успеху современных постоянных угроз (APT) и стали заметной частью крупных нарушений, таких как SolarWinds, в последние годы. Живя за счет наземных угроз, они превосходно умеют оставаться незамеченными и избегать обнаружения, одновременно раскрывая мотивы нападения.

> *Общая тенденция, которую мы наблюдают, было к использованию собственных инструментов для выполнения бесфайловых атак на начальных стадиях до прочная точка опоры и механизм персистентности установлен и безопасен контроль был неполноценный.*

Джеймс Мод,

Ведущий специалист по кибербезопасности Исследователь,

BeyondTrust Labs,

Отчет об угрозах вредоносного ПО 2021 год

Программы-вымогатели побеждают

Атаки программ-вымогателейвырос на 150% в 2020 году , а исследование Tenable сообщает, что35% нарушений теперь связаны с программами-вымогателями .

В ихОтчет об интернет-безопасности за четвертый квартал 2020 г. , WatchGuard Technologies сообщает о росте числа семейств программ-вымогателей на 33% по сравнению с прошлым годом. Почему? Потому что экономика программ-вымогателей продолжает вознаграждать операторов программ-вымогателей.

В соответствии сДелойт , некоторые распространенные предприятия, занимающиеся киберпреступностью, могут вестись всего за 34 доллара в месяц и приносить 25 000 долларов США. Проще говоря, киберпреступность имеет низкий входной барьер в сочетании с потенциально прибыльной рентабельностью инвестиций — и, как правило, все это не облагается налогом!

В 2021 году многочисленные жертвы программ-вымогателей и их страховщики выплатили ошеломляющие семи- и восьмизначные выплаты, в том числе 4,4 миллиона долларов (некоторые из которых впоследствии были возвращены благодаря правительству) компанией Colonial Pipeline и 11 миллионов долларов поставщиком мяса JBS.

Предварительно подготовленные эксплойты и, во все большей степени, программы-вымогатели как услуга (RaaS) упрощают задачу злоумышленникам. Они просто выкладывают несколько долларов (обычно в криптовалюте), указывают и стреляют. С некоторыми инструментами им даже не нужно целиться — вредоносное ПО оппортунистически ищет и проползает через уязвимости везде, где только может с ними столкнуться.**Чтобы окупиться, может потребоваться всего один или два удара.**

6- Отчет об угрозах со стороны программ-вымогателей Unit 42, 2021 г., Palo Alto Networks.

Почему

программы-вымогатели

Победа?

1. Небезопасный удаленный доступ
2. Рискованное поведение пользователей
3. Плохо управляемый привилегированный доступ
4. Неэффективный (или его отсутствие) контроль приложений
5. Неисправленные уязвимости
6. Плохое управление учетными данными

Как склонить чашу весов вспять в борьбе с кибер-злоумышленниками

> В киберпространстве не существует безопасная гавань. Каждая организация с цифровым присутствием обнаженный, как остров среди гневный, неумолимый океан, который кажется, посылает волну за волной кибератаки.

2021 год, пожалуй, выделяется как самый жестокий и шокирующий с точки зрения кибератак. Однако мы также видим некоторые многообещающие признаки того, что ситуацию можно переломить.

президента БайденаИсполнительный указ (EO) об улучшении национальной кибербезопасности Это один из призывов к действию, помогающий мобилизовать ресурсы и сотрудничество в США, и правительства других регионов реагируют аналогичным образом.

В октябре 2021 года США такжесозвал многонациональный саммит на тему борьбы с программами-вымогателями с участием более 30 стран. Поразительные 96% государственного сектора

Руководители ИТ-безопасности заявляют, что их бюджет на кибербезопасность имеет достаточное финансирование, а 83% выражают уверенность в том, что стимул Американского плана спасения (ARP) повысит правительственную кибербезопасность, согласно данным BeyondTrust. Тенденции кибербезопасности 2021 года в правительственном отчете .

Правительственные и регулирующие органы призваны сыграть огромную роль в устранении и судебном преследовании киберпреступников и преступных сетей, а также в разработке стандартов, улучшающих кибербезопасность всей подключенной к Интернету экосистемы.

Более того, правительственные чиновники продемонстрировали новую энергичность в своем подходе к ликвидации синдикатов киберпреступников – независимо от того, поддерживаются ли они заурядными хакерами, стремящимися к прибыли, или субъектами угроз национальному государству.

С учетом вышесказанного, организациям с цифровым присутствием необходимо активно устранять пробелы в безопасности и управлять поверхностью угроз.

Важный сдвиг уже происходит.Безопасность, ориентированная на идентификацию, и нулевое доверие по праву считаются критически важными для защиты от современных, возникающих угроз.

Эти меры контроля могут принести существенные выгоды в виде снижения киберрисков, одновременно делая ИТ-среду более адаптируемой и устойчивой, а также лучше подготовленной к удовлетворению требований будущего.

80% ИТ-безопасности профессионалы говорят переход на удаленку работа увеличивается фокус на безопасность личности

90% ИТ-безопасности плюсы согласились с заявление, *"Личность управление раньше просто был о доступе, сейчас это в основном о безопасность"*

93% ИТ-безопасности профессионалы скажи нулевое доверие является стратегическим для обеспечение моего организация[7]

7. Исследование IDSA: Тенденции в защите цифровых удостоверений 2021 г., IDSA, июнь 2021 г.

7

Информационная безопасность

Выживание

Стратегии

Теперь, когда мы рассмотрели, как работают парадигмы, ландшафт угроз и как меняются тактики киберпреступников, давайте рассмотрим наши основные стратегии ИТ-безопасности и советы по выживанию.

Эти ***7 стратегий***, каждый из которых разбит на советы по выживанию, поможет вам перекалибровать вашу безопасность и лучше защитить ваши данные и цифровые активы.

1

СТРАТЕГИЯ ВЫЖИВАНИЯ

Защитить привилегированных

Личности

Проблема идентификации — самая важная проблема безопасности, которую организациям приходится решать в облачных и локальных средах.

Никакие удостоверения не являются более важными для защиты, чем привилегированные удостоверения, независимо от того, связаны ли они с людьми или машинами, сотрудниками или поставщиками, и являются ли они постоянными или эфемерными.

Учетные данные для этих привилегированных учетных записей могут ускорить доступ к конфиденциальным данным и открыть дополнительные пути, которые позволяют злоумышленнику расширить сферу атаки и повысить привилегии.

Попав в среду жертвы, злоумышленники также могут воспользоваться неадекватными средствами контроля безопасности учетных данных, чтобы захватить дополнительные учетные записи и переместиться в сторону или повысить уровень доступа.**По оценкам Forrester Research, не менее 80% утечек данных подключены к скомпрометированным привилегированным учетным данным.**

Атаки на основе учетных данных (т. е. кража учетных данных, повторное использование паролей, передача хеша и т. д.) по-прежнему остаются ключевым элементом большинства взломов. Яркими примерами являются атаки на «Колониальный трубопровод» и «Веркада». Обе многоэтапные атаки использовали неадекватно управляемые привилегированные учетные данные для получения первоначального доступа в среде жертвы.

Уверенность в обеспечении личности сотрудников резко упал, падение с 49% в 2020 году до лишь 32% в 2021 году.[8]

8- Тенденции в области защиты цифровых удостоверений на 2021 год. ИДСА. Июнь 2021.

Злоумышленники Verkada обнаружили учетные данные суперадминистратора, встроенные в скрипт Python в общедоступном плагине Veracode Jenkins на сервере Verkada.

Эти учетные данные должны были быть заменены (например, с помощью вызова API) и сохранены с помощью решения для управления привилегированными паролями.

В случае взлома Colonial Pipeline группа киберпреступников Darkside обнаружила украденные учетные данные, которые обеспечивали доступ к неактивной учетной записи Colonial Pipeline VPN, которая все еще была подключена к сети. Вполне вероятно, что учетные данные, найденные Darkside, были повторно использованы в нескольких системах.

Эту раннюю стадию атаки можно было бы легко предотвратить с помощью как минимум трех различных элементов управления привилегированными паролями:

1. Обеспечение использования уникальных учетных данных для предотвращения использования скомпрометированных учетных данных для нескольких учетных записей и активов.
2. Частая смена учетных данных для ограничения времени, в течение которого украденный пароль остается активным и может быть использован для получения доступа.
3. Обзор привилегированного доступа; полученные результаты могли бы побудить команды безопасности либо отключить неактивную учетную запись VPN, внедрить дополнительные рабочие процессы для ее использования, либо внедрить оповещения о ее использовании, чтобы обеспечить тщательный мониторинг.

Вотчет По данным Альянса безопасности с определением личности (IDSA), своевременные проверки привилегированного доступа на самом деле были наиболее часто упоминаемым (50% респондентов) средством контроля безопасности, которое могло бы предотвратить или смягчить взлом, с которым столкнулись респонденты.

Часто по умолчанию предоставляется слишком большой доступ или доступ является открытым (постоянные привилегии), когда его следует предоставлять только вовремя, когда выполняются определенные контекстные параметры, а затем отзывать после завершения задачи. изменился контекст или прошло определенное количество времени.

Расползание привилегий — еще один риск, который легко не заметить. Роли меняются, люди накапливают привилегии или покидают компанию, но доступ и учетные записи остаются активными. Регулярно пересматривая использование доступа и роли, вы можете точно настроить предоставление ресурсов, чтобы обеспечить соблюдение в организации принципа наименьших привилегий (PoLP).

Например, если учетная запись с привилегированным доступом не использовалась в течение месяца, возможно, она больше не нужна и ее можно удалить, что исключает риск. Или, если учетная запись используется редко и только для действий с очень высоким уровнем привилегий, возможно, имеет смысл включить дополнительные рабочие процессы, чтобы разрешить использование учетной записи и отправлять оповещения другим, когда учетная запись используется. Это позволит ему получить более пристальное наблюдение.

Даже при отсутствии трех упомянутых выше мер контроля атаку Colonial Pipeline все равно можно было бы предотвратить на многих этапах, особенно с помощью средств управления привилегиями конечных точек, которые включают в себя обеспечение минимальных привилегий и контроль приложений. Да, нарушения могут произойти, и часто злоумышленникам нужен только один путь, но многие привилегированные доступы и другие средства контроля обычно должны отсутствовать или применяться неправильно, чтобы атака достигла разрушительного уровня нарушения Колониального трубопровода.

Некоторые нечеловеческие (также называемые машинными) учетные записи, например учетные записи служб, играют решающую роль в запуске программ, приложений и рабочих процессов автоматизации. Учетными записями компьютеров, используемыми для автоматизации, может быть особенно сложно или невозможно управлять вручную из-за потенциального влияния на время безотказной работы, если распространение изменения пароля не будет быстро синхронизировано во всех местах, где ссылается на учетную запись. Таким образом, многие организации вообще пренебрегают управлением этими учетными записями, надеясь, что другие уровни помешают злоумышленнику получить доступ к учетной записи.

Нечеловеческим учетным записям часто предоставляются чрезмерные привилегии. Инструменты DevOps и рабочие процессы CI/CD создают схожие проблемы и риски.

Чтобы предотвратить взлом учетных записей, организации должны автоматизировать и централизовать жизненные циклы привилегированных учетных данных, ключей и секретов.

СОВЕТЫ ПО ВЫЖИВАНИЮ

Автоматизируйте обнаружение и регистрацию всех привилегированных удостоверений.(человек/приложение/машина) и активы, чтобы устранить «слепые зоны» привилегий и взять под контроль теневые ИТ.

Храните и управляйте всеми привилегированными учетными данными(пароли, ключи и секреты) в соответствии с рекомендациями по обеспечению безопасности паролей. Эти методы должны включать обеспечение сложности и уникальности паролей, ротацию учетных данных и внедрение их непосредственно в сеансы, никогда не раскрывая их конечному пользователю, будь то сотрудник, поставщик или машина. Обеспечение соблюдения таких возможностей, как уникальные пароли иротация паролей, помогают предотвратить атаки по подбору пароля, а также атаки повторного использования. При ротации (изменении) учетных данных, например, после каждого использования в случае одноразовых паролей (OTP) и динамических секретов, даже если пароль был скомпрометирован, срок его действия истекает к моменту, когда злоумышленник пытается его использовать.

Внедрение адаптивного контроля доступа, одобряя или запрещая запросы на доступ «точно в срок» на основе контекста и отзыв доступа после завершения действия, изменения контекста или прохождения определенного периода времени. Модель доступа JIT исключает открытый привилегированный доступ, значительно сокращая время, в течение которого учетная запись является привилегированной, и, таким образом, представляет риск вектора привилегированной атаки. Однако учетные записи служб не следует делегировать какой-либо модели доступа JIT.

Постоянно отслеживайте привилегированные учетные записи и любые сеансы, связанные с привилегированной деятельностью., будь то человеком, приложением или машиной. Мониторинг должен включать в себя запись экрана, регистрацию команд, выполнение сценариев и вывод данных на экран. Аномальная активность должна отмечаться с возможностью выявления, приостановки и прекращения подозрительных сеансов в режиме реального времени. Привилегированный доступ также должен периодически пересматриваться, чтобы при необходимости можно было вносить коррективы в доступ, а также в его мониторинг.

Принудительно использовать многофакторную аутентификацию (MFA)во время входа в систему, при проверке пароля и при повышении привилегий — в любое время при появлении нового запроса. Это обеспечивает дополнительную уверенность в том, что личность, участвующая в привилегированном сеансе, является тем, кем она себя называет и кем вы ожидаете от нее быть.

Удаление общих учетных записейдля обеспечения четкого контроля и возможности аудита действий пользователей, выполняемых каждым пользователем и связанными с ним учетными записями. Когда присутствуют общие учетные записи, это запутывает контрольный журнал и может сделать невозможным узнать, кто и что сделал с учетной записью. Общие учетные записи также могут усложнить реализацию различных инициатив по обеспечению соответствия.

Уничтожьте встроенные паролив IoT и других устройствах, приложениях, сценариях и инструментах DevOps и замените их безопасными вызовами API или динамическими секретами. Такая практика устранила бы вектор угрозы встроенного скрипта Python, который позволил злоумышленникам Verkada закрепиться.

Ключевой вывод

Многие из вышеперечисленных средств защиты, такие как MFA, своевременный доступ, адаптивный доступ и непрерывный мониторинг, также помогут обеспечить нулевое доверие.

86%лиц, принимающих решения в области ИТ и безопасности говорят, что они вкладывают больше средств в PIM (управление привилегированными идентификационными данными) ближайшие два года для устранения рисков связанные с удаленной работой.[9]

9. Развитие управления привилегированными идентификационными данными (PIM) в «следующей нормальности». Forrester Consulting (по заказу BeyondTrust), ноябрь 2020 г.

2

СТРАТЕГИЯ ВЫЖИВАНИЯ

Безопасный удаленный доступ

Доступ к конфиденциальным ресурсам, плоскостям управления (облако, виртуализация, DevOps) или выполнение привилегированных действий должен быть заблокирован и тщательно контролироваться, чтобы не подвергаться перебору и другим атакам.

Еще одна проблема заключается в том, что когда учетные данные вводятся удаленно, они подвергаются воздействию локального компьютера, а также любому вредоносному ПО или атаке (например, «человек посередине»), которые могут их перехватить.

В конечном счете, путь к решению этих проблем предполагает распространение лучших практик управления привилегированным доступом (наименьшие привилегии, управление привилегированными паролями, мониторинг/управление сеансами и т. д.) за пределы периметра.

Традиционный пульт технологии доступа (VPN, RDP, VNC и т. д.) отсутствие детального доступа элементы управления и сеанс видимость, создание опасная безопасность отверстия при выдвижении многие из сегодняшних удаленных рабочие варианты использования.

В феврале 2021 года водоочистная станция во Флориде (Олдсмар) была взломана удаленно, и злоумышленник попытался изменить химический состав воды. Исследователи изCyberNews обнаружил 11 взломанных учетных данных связан с водоочистной станцией с 2017 года, а также 13 комплектов учетных данных прямо перед атакой.

Судя по всему, все компьютеры имели один и тот же пароль для удаленного доступа и были подключены напрямую к Интернету без какой-либо защиты брандмауэра. Злоумышленник также воспользовался одним из инструментов удаленного доступа потребительского уровня, чтобы получить доступ к системам управления SCADA завода, а затем изменил уровень гидроксида натрия в воде (широко известного как щелок) со 100 частей на миллион до 11 100 частей на миллион. миллион.

Завод фактически прекратил использовать инструмент удаленного доступа TeamViewer шесть месяцев назад, но все же оставил его установленным. К счастью, оператор завода вовремя заметил изменение и отменил его до того, как нарушение поставило под угрозу здоровье населения.

СОВЕТЫ ПО ВЫЖИВАНИЮ

Посредничество всех соединений через единый путь доступа, шифровать весь трафик и делать каждое удаленное соединение исходящим. Эти элементы управления помогают свести к минимуму количество попыток входа в систему, одновременно сохраняя дистанцию между удаленным доступом и интернет-угрозами.

Прокси-доступ к плоскостям управления и другому критически важному программному обеспечениюсегментировать и изолировать трафик удаленного доступа. Кроме того, доступ администратора должен быть доступен только авторизованным администраторам.

Обеспечить зонирование и сегментацию сетиизолировать и защитить новые поверхности атак, созданные в результате цифровой трансформации и развертывания облачных технологий. Это также помогает гарантировать, что конфиденциальное программное обеспечение, приложения и среды не посягают друг на друга.

Обеспечьте контроль доступа с наименьшими привилегиями,с своевременной подготовкой для любого удаленного доступа. Это мощная и необходимая способность не дать злоумышленникам и вредоносным программам закрепиться, а также совершить боковое движение. Ограничение привилегий до необходимого минимума также помогает обеспечить честность поставщиков и других удаленных работников, поскольку они могут получить доступ только к тому, что им необходимо для выполнения своей работы.

Автоматически внедрять управляемые учетные данныев удаленные сеансы, чтобы конечные пользователи никогда не узнали или не прикоснулись к учетным данным для входа. Это помогает обеспечить использование надежных методов защиты паролей для всех конфиденциальных удаленных сеансов, даже для поставщиков/третьих сторон.

- **Внедрить управление BYOD**обеспечить безопасность устройств путем изоляции и защиты приложений и контента, к которым осуществляется доступ в рабочей области. Это требует перехода от управления мобильными устройствами (MDM) к управлению мобильностью предприятия (EMM), которое может защитить не только устройство, но также отдельные приложения и данные, содержащиеся в нем.

- **Обеспечьте микросегментацию на уровне приложения.**это не позволяет удаленным работникам и поставщикам обнаруживать или выполнять приложения и другие ресурсы, к которым у них нет доступа.

- **Отслеживайте, управляйте и проверяйте каждый удаленно инициированный привилегированный сеанс.**посредством записи экрана, регистрации нажатий клавиш и других технологий. Это обеспечивает высокий уровень контроля и защиты, которого крайне не хватает VPN и другим технологиям удаленного доступа, гарантируя, что вы всегда знаете, какая личность входит в систему удаленно и что они делают с этим доступом.

Ключевой вывод

Применение многих из этих практик не только значительно снизит риск вашей организации предоставить злоумышленникам легкую точку опоры в вашей среде, но также обеспечит мощную защиту от горизонтального перемещения. Кроме того, каждый из этих советов является важным компонентом реализации архитектуры нулевого доверия для удаленного доступа.

9. Развитие управления привилегированными идентификационными данными (PIM) в «следующей нормальности». Forrester Consulting (по заказу BeyondTrust), ноябрь 2020 г.

3

СТРАТЕГИЯ ВЫЖИВАНИЯ

Применить управление привилегиями конечных точек

(Наименьшие привилегии и контроль приложений)

Позиция безопасности с наименьшими привилегиями может не только полностью исключить возможность выполнения и закрепления многих типов вредоносного ПО и других атак, но также может загнать в тупик злоумышленников, которые все же закрепились, резко снижая вероятность повышения привилегий и горизонтального движения, ключевых этапов цепочка кибератак.

70% атак сегодня Сообщается, что они связаны с той или иной формой бокового движения.[10]

Ограничение привилегий программного обеспечения и системы минимальным набором процессов, необходимых для выполнения авторизованной деятельности, также снижает вероятность возникновения проблем несовместимости; защищает организации от мошеннических, скомпрометированных или неправильно используемых приложений; и снижает риск простоев, улучшая общие эксплуатационные характеристики.

Применяя принцип наименьшие привилегии (PoLP) — один из самых мощных и общепризнанные способы предотвратить заражение вредоносным ПО, защитить от внутренних и внешние субъекты угроз и уменьшить потенциальный ущерб от инцидента безопасности.

10- Отчет EGlobal об угрозах реагирования на инциденты, Технический углерод.

В 2020 годуВеркада разоблачена прямые трансляции со 150 000 камер видеонаблюдения, используемых их клиентами, включая тюрьмы, больницы, женские клиники, психиатрические учреждения, полицейские управления и даже такие компании, как Tesla. Как подробно говорилось ранее, взлом Verkada произошел из-за скомпрометированных учетных данных суперадминистратора, которые были обнаружены встроенными в скрипт Python, к которому был доступен удаленный доступ. Злоумышленники получили «root» доступ к камерам Verkada с помощью встроенных функций, которые повысили их привилегии до «Суперадминистратора». Эта учетная запись суперпользователя/root давала доступ ко всем камерам клиентов Verkada, что потенциально ставило под угрозу безопасность и конфиденциальность в каждой среде клиента.

Многие элементы управления с наименьшими привилегиями (удаление прав администратора и т. д.) помогли бы предотвратить или смягчить это нарушение, равно как и принудительное разделение привилегий и обязанностей. Ни одна учетная запись не должна контролировать такое количество различных учетных записей клиентов и иметь такие привилегии высокого уровня в таком количестве систем. Вместо того, чтобы одна учетная запись суперпользователя выполняла все обязанности ИТ-администратора, реализуйте разделение привилегий и обязанностей между разными учетными записями, при этом каждая учетная запись требует уникальных учетных данных для входа и используется только для определенного набора функций/задач.

СОВЕТЫ ПО ВЫЖИВАНИЮ

Обеспечьте соблюдение минимальных привилегий в вашей среде.Устраните права локального администратора, права администратора сервера, права системы и приложения до минимально необходимого уровня. Доступ должен детально контролироваться и повышаться только в нужный момент. Наименьшие привилегии должны применяться ко всем конечным точкам (Windows, Mac, Unix, Linux, сетевым устройствам и т. д.), а также к локальным, облачным и гибридным средам. Отказ от прав администратора сам по себе приводит к значительному снижению рисков на многих платформах, даже при отсутствии соответствующего процесса установки исправлений. Как мы опубликовали в нашем отчете об уязвимостях Microsoft за 2021 год, в 2020 году 56% всех критических уязвимостей Microsoft и 87% критических уязвимостей в Internet Explorer и Edge можно было бы устранить путем удаления прав администратора.

Назначайте определенные команды Unix и Linuxчто ИТ-администраторы могут выполнять и запускать с повышенными правами без необходимости использования sudo или root. Также обеспечьте фильтрацию командной строки и язык политики, который может повышать уровень команд с минимальными привилегиями и проверять все параметры и переключатели. Это позволяет выявлять неправильно сформированные или неподходящие команды, которые могут привести к простою критически важного программного обеспечения и раскрыть векторы атак, которыми можно воспользоваться.

Обеспечьте разделение обязанностей и разделение привилегийдля ограничения привилегий, связанных с любой учетной записью или процессом. Применительно к пользователям это предполагает сегментирование привилегий между отдельными пользователями и учетными записями, а также обеспечение возможности выполнения определенных обязанностей только с использованием определенных учетных записей и удостоверений. Таким образом, если одна учетная запись скомпрометирована, диапазон привилегий, которые она предоставляет злоумышленнику, ограничивается. Разделение привилегий помогает сдерживать злоумышленников вблизи точки компрометации и ограничивает горизонтальное перемещение.

Применяйте расширенный контроль приложений и управление приложениями с минимальными привилегиями.чтобы гарантировать, что только утвержденные приложения и разрешенные подфункции этих приложений могут работать в правильном контексте. Благодаря наложению контроля приложений поверх управления привилегиями критически важные функции операционной системы по умолчанию считаются доверенными (пользователи без привилегий не могут вводить новый код в такие каталоги, как Program Files, Windows, System32 или Drivers). Это делает этот подход прагматичным, поскольку его необходимо применять только к конкретным каталогам и файлам, куда злоумышленники обычно «сбрасывают» и выполняют свои полезные данные. Этот тип контроля также предотвратит выполнение в системе неподписанных двоичных файлов, что используется в атаках вредоносного ПО Darkside.

Защита от неправомерного использования доверенных приложенийпутем применения элементов управления безопасностью привилегированного доступа contextrich, таких как правила контроля контента и приложений, а также контроля над запуском дочерних процессов. Это помогает защититься от сложных бесфайловых атак, часто являющихся частью сложных постоянных угроз и изощренных атак (SolarWinds, Darkside и т. д.), в которых используются Powershell, Wscript, Csript, Word и другие законные инструменты.

Ключевой вывод

Большинство из этих элементов управления с минимальными привилегиями имеют решающее значение для создания среды с нулевым доверием. В прошлом году многие из вышеперечисленных мер контроля помогли бы пресечь крупномасштабные атаки на нескольких этапах, включая атаки Colonial Pipeline и Verkada, а также бесчисленное множество более мелких нарушений и инцидентов, связанных с безопасностью.

Атака на цепочку поставок SolarWinds Orion была особенно разрушительной, поскольку приложению Orion требовался неограниченный доступ к работе. Поскольку само приложение Orion было скомпрометировано, злоумышленники воспользовались этим неограниченным привилегированным доступом ко всем средам жертв, использующим это приложение.

Эта атака демонстрирует, почему организациям важно выявлять и устранять приложения с чрезмерными привилегиями и, где это возможно, внедрять управление приложениями с наименьшими привилегиями.

Однако, поскольку многие устаревшие приложения (например, SolarWinds Orion) могут не работать без этих высоких уровней привилегий, предприятиям и агентствам следует либо внедрить дополнительные уровни защиты, либо прекратить использование программного обеспечения.

4

СТРАТЕГИЯ ВЫЖИВАНИЯ

Нанесите закалку и Управление уязвимостями

Удаленные конечные точки и конечные точки BYOD представляют собой серьезную проблему безопасности с точки зрения реализации конфигураций, элементов управления и исправлений.

Однако обеспечение минимальных привилегий и удаление прав администратора, как описано ранее, является важным элементом контроля, который может помочь снизить эти риски.

Спеша поддержать большая удаленная рабочая сила в первые дни пандемия COVID-19, агентства и предприятия ослабил их закалку политика.

СОВЕТЫ ПО ВЫЖИВАНИЮ

Укрепите свою ИТ-среду.Удалите ненужное программное обеспечение, приложения и привилегии, закройте ненужные порты и убедитесь, что на конечных точках установлены последние версии встроенного ПО и исправлений. В идеале это делается до того, как конечной точке будет предоставлен доступ к вашей сети. Действия по усилению защиты следует продолжать выполнять по мере необходимости на протяжении всего жизненного цикла устройства и обеспечивать надежные базовые конфигурации. Это особенно важно, поскольку устройства могут вернуться в офис после пребывания дома во время карантина по коронавирусу.

Укрепите и защитите BIOS.Это должно повлечь за собой включение защиты паролем для BIOS и обеспечение надежности, сложности и, самое главное, уникальности пароля. Более того, загрузочное устройство должно быть настроено на загрузку только с внутреннего жесткого диска с использованием UEFI и безопасной загрузки, а не с внешнего носителя, такого как USB-устройство. Внешнее загрузочное устройство может обойти другие меры безопасности и даже перезаписать операционную систему. Таким образом, он будет контролировать загрузку устройства и не забудет использовать пароль BIOS для защиты этой настройки. Паролем BIOS можно управлять с помощью привилегированного решения для управления паролями.

Внедрить непрерывное управление уязвимостями.Постоянно сканируйте, оценивайте, расставляйте приоритеты и устраняйте уязвимости программного обеспечения, приложений и других систем. Устранение уязвимостей может повлечь за собой исправление и/или другое смягчение последствий (т. е. изменение конфигурации или использование инструментов кибербезопасности), тогда как принятие уязвимости может включать в себя действия, варьирующиеся от бездействия до приобретения киберстраховки. Расстановка приоритетов является ключевым компонентом управления уязвимостями и необходима для эффективного устранения огромного множества уязвимостей, которые могут существовать в любой умеренно сложной ИТ-среде. Хотя установка исправлений гарантированно устранит или «исправит» уязвимость, сама по себе установка исправлений не всегда является безрисковой деятельностью — она может вызвать несовместимость, сбой в работе программного обеспечения или даже привести приложение или инструмент к несоответствию требованиям. Вот почему ИТ-командам следует искать автоматизированные инструменты, которые помогут им быстро принимать разумные решения по управлению уязвимостями, которые минимизируют поверхность атаки, сохраняя при этом время безотказной работы.

Ключевой вывод

В совокупности усиление защиты систем, управление конфигурацией и управление уязвимостями могут обеспечить надежную основу для защиты программного обеспечения и конечных точек.

5

СТРАТЕГИЯ ВЫЖИВАНИЯ

Предотвратить вмешательство мобильных и удаленных конечных точек

За пределами корпоративных среды, мобильные и удаленные конечные точки более подвержены атаки на устройства.

Хотя некоторые устройства могут быть украдены просто в рамках обычной кражи со взломом, целью которой являются ценные предметы, национальные государства и другие организованные субъекты угроз могут атаковать дома привилегированных пользователей в рамках кибершпионажа. Обеспечение целостности удаленных и мобильных конечных точек, а также данных, находящихся на них, имеет решающее значение.

СОВЕТЫ ПО ВЫЖИВАНИЮ

Внедрить шифрование диска. Это лучший способ гарантировать, что злоумышленник не сможет получить доступ к конфиденциальным данным в случае удаления жесткого диска. Даже если устройство снято и установлено на внешнем оборудовании, к нему не будет легко получить доступ, поскольку шифрование обычно сочетается с исходным оборудованием. А если устройство физически украдено, без пароля доступ все равно запрещен. Однако обратите внимание, что для некоторых устройств для расшифровки диска и предоставления доступа достаточно пароля или ключа администратора.

Используйте встроенные жесткие диски.Они становятся все более распространенными, чтобы сократить расходы на устройства и позволить использовать легкие ноутбуки. Этот носитель данных не является съемным, как жесткий диск PCIe или SATA, а скорее микрочипы для хранения SSD физически припаяны к материнской плате. Обратной стороной является то, что такая практика может затруднить законное обслуживание устройства или обновление хранилища.

Загерметизируйте устройство.Винты, скрепляющие устройство, могут варьироваться от Phillips до Torx. Некоторые размеры являются стандартными, а другие являются запатентованными. Как бы тривиально это ни звучало, если у злоумышленника нет инструментов для открытия устройства, у него меньше шансов получить доступ. Это особенно актуально, если их доступ к устройству происходит в течение короткого промежутка времени. А если винты заклеены клеем или связующим веществом, их нелегко удалить, что делает устройство практически одноразовым в случае неисправности. Это справедливо для любого устройства, которое пользователю может понадобиться при удаленной работе — от ноутбука до аппаратного VPN.

Если внутренние компоненты устройства представляют собой риск, а модель риска, неисправности и стоимости оправдывает это, рассмотрите возможность постоянной изоляции устройства от любого доступа.

Раздавать и требовать использования кабелей компьютерной безопасности.чтобы закрепить устройство на столе во избежание кражи. Кабели компьютерной безопасности состоят из троса, замка (комбинации или ключа) и монтажного зажима, который прикрепляется к защищаемому активу с помощью овального разъема стандартного размера. Кабели безопасности обычно используются в местах с интенсивным пешеходным движением или в общественных местах, но они также обеспечивают эффективный уровень физической защиты для домашних/удаленных офисов. Если конечная точка, используемая в доме сотрудника, содержит конфиденциальную информацию, рассмотрите возможность выдачи пользователю защитных кабелей, чтобы предотвратить кражу.

Примените защиту от несанкционированного доступа BIOS.*Примечание. Эта функция доступна только у определенных поставщиков.*Защита от несанкционированного доступа обычно включается в BIOS и имеет программный компонент, загружаемый в операционную систему. Защита от несанкционированного доступа контролирует устройство на наличие признаков того, что корпус устройства был открыт или физические компоненты были удалены или заменены. Если обнаружено несанкционированное вмешательство, программное обеспечение предупреждает платформу управления. Защиту от несанкционированного доступа к BIOS следует считать важной технологией для мобильных устройств, используемых удаленными работниками. При отсутствии защиты от несанкционированного доступа рассмотрите возможность создания дельта-отчетов по оборудованию с помощью систем управления активами, чтобы определить, были ли изменены, удалены или добавлены какие-либо компоненты. Хотя это не скажет вам, был ли корпус открыт ненадлежащим образом, это поможет определить, были ли изменены ключевые компоненты.

Ключевой вывод

Поскольку для работы используются тысячи и миллионы удаленных и мобильных конечных точек (как корпоративных, так и принадлежащих сотрудникам), вероятность кражи или потери устройства высока. Сочетание этих средств защиты от несанкционированного доступа в сочетании с четкой и строгой политикой в отношении устройств, о которой пользователи хорошо осведомлены, имеет решающее значение для предотвращения и смягчения последствий кражи и/или взлома устройств.

6

СТРАТЕГИЯ ВЫЖИВАНИЯ

Безопасность и расширение возможностей

Служба поддержки

На начальных этапах пандемии и социального дистанцирования службы поддержки делали все, что могли, используя имеющиеся у них инструменты, чтобы помочь своим организациям перейти на удаленную работу, но зачастую это было не очень приятно.

А поскольку все пользователи недавно начали работать из дома и часто используют новые инструменты, количество обращений в службу поддержки резко возросло.

Хотя многие из инструментов службы поддержки, использованные для новых сценариев использования, создавали проблемы с масштабируемостью, их риски для безопасности вызывают гораздо большую озабоченность.

Многие организации не осознали того факта, что удаленная поддержка представляет собой тип привилегированного доступа и к ней следует относиться соответственно. Например, специалистам службы поддержки часто требуется использовать учетные данные администратора с повышенными привилегиями для решения проблем поддержки.

По мере роста числа случаев использования удаленной поддержки и автоматического доступа растет и риск безопасности. Компрометация инструмента удаленной поддержки/доступа потребительского уровня привела к взлому, в результате которого была предпринята попытка отравления воды на водоочистной станции Олдсмар во Флориде.

Службам поддержки требуется инструмент удаленной поддержки, который постоянно защищает их и клиентов (как внутренних, так и внешних), которые они обслуживают, сокращает время обработки инцидентов, повышает удовлетворенность клиентов и разрешение первых обращений, оптимизирует процессы и обеспечивает синергию с другими инструментами службы поддержки, которые они используют.

Пандемия бросила вызов люди во всех отраслях, некоторые больше, чем другие. В мире ИТ, пожалуй, ни одна группа не имела большей тяги на его тарелке, и не было более имеет решающее значение для компании способность адаптироваться, чем сервисная стойка.

В дальнейшем сервис столы будут продолжать сильно опираться и будет играть решающую роль в сохранении организаций безопасный.

СОВЕТЫ ПО ВЫЖИВАНИЮ

Обеспечьте строгий контроль безопасности привилегированного доступа для всех сеансов удаленной поддержки.Сеансы должны иметь надежное шифрование. Инструмент удаленной поддержки должен иметь возможность работать через брандмауэры без туннелирования VPN, чтобы безопасность вашего периметра оставалась неизменной. Используя только исходящий сеансовый трафик, например TCP-порт 443, вы также можете свести к минимуму воздействие на порт, значительно сужая потенциально уязвимую поверхность атаки вашего сайта поддержки.

Примените сегментацию клиентов.Каждый клиент удаленной поддержки должен быть сегментирован через однопользовательскую среду, чтобы данные никогда не смешивались.

Внедрите лучшие практики обеспечения безопасности учетных данных.Включите MFA и управляйте всеми учетными данными в хранилище. Учетные данные должны автоматически вводиться в сеансы, не раскрываясь пользователю или персоналу удаленной поддержки. Также желательно применять разные политики для автоматического и контролируемого доступа.

Включите независимую от платформы поддержку.Технические специалисты службы поддержки должны иметь возможность оказывать поддержку независимо от своей платформы или платформы конечного пользователя. Чем шире поддержка платформы, тем больше шансов на стандартизацию поддержки за счет использования единого инструмента для сокращения времени обработки инцидентов, повышения производительности технических специалистов и получения других преимуществ.

Оптимизируйте рабочие процессы и интегрируйтесь с другими инструментами службы поддержки.чтобы обеспечить удобство работы как для технического специалиста, так и для клиента. Ваши технические специалисты должны иметь возможность запускать сеанс удаленной поддержки непосредственно из заявки в службу поддержки или записи изменения, автоматически обновлять заявки с подробностями сеанса поддержки и включать в заявку расшифровку чата и запись сеанса.

Наконец, развернув управление привилегиями конечных точек в сочетании с вашим инструментом удаленной поддержки,вы можете резко сократить количество обращений к ИТ-специалистам и разгрузить службу поддержки, помогая им масштабироваться и работать с максимальной эффективностью.

7

СТРАТЕГИЯ ВЫЖИВАНИЯ

Выполнение удаленного работника

Проверка на проницаемость,

Осторожно

Проблемные или недопустимые тесты на проникновение для удаленных сотрудников

Во-первых, давайте рассмотрим типы ресурсов и сценариев, которые обычно выходят за рамки любого корпоративного удаленного тестирования на проникновение.

ОБЪЕКТ	СЦЕНАРИЙ
Личное, Домашний Сети	Проводное и беспроводное соединение, включая разведку сети и инвентаризацию устройств. Чтобы провести тестирование на проникновение в эти области, вам необходимо получить явное разрешение от конечного пользователя на инвентаризацию, классификацию и анализ рисков в сетях, поддерживающих его домашнюю среду. Политика компании также должна позволять проведение такого тестирования. Большинство домашних пользователей отклонят этот запрос на доступ.
Устройства принадлежат Другие Компании	Возможно, вы используете одну и ту же сеть, проводную или беспроводную, поскольку другие члены семьи работают дома. Это явно представляет собой проблему масштабирования и никогда не должен допускаться для каких-либо проверок на проникновение.

Удаленные работники меняются поверхность атаки и создавать новые риски, которые необходимо оценить.

Но что представляет собой действительный тест на проникновение для конечного пользователя (тест на проникновение), когда цель находится не в физический офис?

Что именно ты разрешили протестировать?

Персональные устройства вне пределов?

Вы также должны рассмотреть какие у тебя разрешения возможно, потребуется получить если твое проникновение испытание выходит за рамки оборудование, которое вы выпустили, и электронно перемещается домашние сети и потребительский интернет провайдеры.

Личное и
Интернет вещей

Включая персональных цифровых помощников, системы сигнализации, домашнюю автоматизацию и т. д. Такие устройства и программное обеспечение представляют собой потенциальный критический вектор атаки, например, со стороны уязвимых устройств с истекшим сроком эксплуатации. Корпоративная оценка этих устройств допускается только с явного разрешения сотрудника/владельца устройства. Кроме того, имейте в виду, что цель (устройство и т. д.) может оказаться неработоспособной в результате агрессивной проверки на проникновение.

Личное электронное письмо
адреса
это может быть
на том же самом
BYOD-активы

Это запрещено, независимо от того, где находится личное устройство. Организациям следует обеспечить использование решений MDM или EMM для обеспечения сегментации электронной почты и управления данными.

Домашний телефон
Числа

Также может использоваться другими членами того же домохозяйства, что и работник. Сможет ли кто-нибудь, кроме сотрудника, ответить на звонок, если он зазвонит? Не проводите проверку на проникновение, если вы не можете с высокой степенью достоверности предсказать личность получателя звонка.

Мобильный телефон
Числа

При использовании для ответа на рабочие звонки это серая зона проверки пера. Если владелец устройства тратит деньги на свой мобильный телефон, это BYOD для бизнеса и честная игра для проверки пера в обычные рабочие часы. Тем не менее, это по-прежнему личное устройство, и необходимо учитывать область применения — от вишинга до SMishing (голосовой и SMS-фишинг) — в зависимости от политики кодекса поведения вашего бизнеса и региональных законов.

Неделовой
Социальные медиа
Счета

Это не изменилось для удаленных работников и не должно рассматриваться как часть какой-либо новой политики и сферы применения.

Хотя любой вектор из приведенного выше списка может быть использован злоумышленником, они, как правило, закрыты или, по крайней мере, проблематичны для проверки на проникновение из-за юридических разветвлений, юрисдикции, собственности, собственности и/или местных законов. В этих случаях организации могут законно проводить пен-тесты только в том случае, если целевой сотрудник дал явное согласие. Маловероятно, что ваш кодекс поведения и политика безопасности вашего сотрудника содержат положения, позволяющие проводить пен-тесты для вышеуказанных случаев использования.

Самые допустимые пен-тесты на предмет рисков, связанных с удаленными работниками

Теперь, когда мы рассмотрели пен-тесты, которые, скорее всего, противоречат политике компании, давайте рассмотрим действенные методы тестирования на проникновение удаленных сотрудников.

ТИП АТАКИ	ДЕЙСТВИТЕЛЬНЫЙ МЕТОД ТЕСТИРОВАНИЯ
Фишинг	Пен-тестирование с использованием фишинга должно быть нацелено на всех пользователей независимо от их роли — от руководителя до секретаря, от штатных сотрудников до новых сотрудников. Веб-почта, мобильные устройства и почтовые клиенты — все это честная игра. В рамки фишинг-тестов могут также входить специализированные атаки, такие как целевой фишинг и китобойная атака. Рассмотрите возможность не объявлять заранее о фишинговых тестах на проникновение и, возможно, оставьте их доступными для всех пользователей, оставив права на ознакомление только с ключевыми сотрудниками, которые могут рассортировать попытки фишинга, идентифицированные конечным пользователем.
Вишинг	Социальная инженерия, которая нацелена на пользователей посредством телефонных звонков на стационарные телефоны, сотовые телефоны, VoIP, телефонные системы и приложения, а также домашние телефоны POTS (простая старая телефонная система). В зависимости от того, как конечный пользователь принимает телефонные звонки (и гарантирует, что на звонок отвечает только он), вишинг дает оценку риска того, как вербальная социальная инженерия может быть использована против бизнеса. Пентестеры Вишинга могут выдавать себя за клиентов, продавцов или других сотрудников, попавших в беду или нуждающихся в информации.

смишинг

Социальная инженерия с использованием текстовых SMS-сообщений. SMishing является эффективным вторичным вектором атаки, когда он замаскирован под двухфакторную аутентификацию или когда CallerID подделывается так, будто он исходит от известного абонента (например, от основной телефонной линии организации) или от местного номера телефона. На самом деле SMishing имеет только два вектора атаки для пентестера: ответ на текст или нажатие на ссылку. Хотя ответы на попытки SMishing могут раскрывать конфиденциальную информацию, ссылки, ведущие на фальшивые страницы аутентификации, как правило, работают лучше всего при попытке эксплуатировать пользователей. Эти тесты на проникновение будут проводиться на зарегистрированных мобильных устройствах, которым разрешено обрабатывать рабочие звонки и электронные письма.
Если устройство действительно личное и телефон не зарегистрирован в корпоративном каталоге, вероятно, оно выходит за рамки вашей компетенции.

Социальное
СМИ для
Продвигать
Работа

Использование сотрудниками для продвижения рабочих мероприятий, продаж, новостей и активности — это честная игра для проверки пера, независимо от того, работает ли целевой сотрудник из дома или нет. Все, что нужно сделать пентестерам, — это ответить на существующее сообщение, связанное с работой, чтобы начать атаку. Честно говоря, вы, вероятно, обнаружите, что обучение конечных пользователей этому методу атаки так же важно, как и фишингу по электронной почте, особенно если пользователи очень активны в социальных сетях от имени организации.

Удаленный
Доступ
Инфраструктура

Охватывает все: от VPN-клиентов до VPN-концентраторов и специальной технологии удаленного доступа, используемой удаленными работниками для доступа к ресурсам. Не сообщайте пентестеру топологию сети для удаленного доступа. Вы хотите, чтобы пентестер попытался определить поставщиков, сети и процессы для удаленного доступа. Если пентестер может выполнить такое сопоставление, то все, что ему нужно сделать, — это использовать социальную инженерию или комбинацию уязвимостей и эксплойтов, основанную на поставщике или технологии, для проникновения в организацию. Если злоумышленник понимает, как ваши удаленные сотрудники получают доступ на детальном уровне, это лишь вопрос времени, когда они найдут уязвимость и воспользуются ею.

Удаленный конец

Пользователи на

Компания-

Собственные активы

Действительная цель для пен-теста, независимо от того, находятся ли они локально или работают удаленно. Возможно, вам не будет разрешено сканировать устройство через домашнюю сеть пользователя, но вы, безусловно, можете сканировать устройство, если существует сетевое туннельное соединение на основе протокола. Метод сканирования имеет значение. Если вы можете удаленно эксплуатировать конечного пользователя через VPN, то цель пентестера достигнута. Хотя горизонтальное перемещение к домашним устройствам посредством тестирования на проникновение обычно недопустимо, горизонтальное перемещение к другим видимым устройствам через VPN разрешено (за исключением атак с раздельным туннелированием). Проверка на проникновение должна проводиться в пределах корпоративной сети, включая туннели VPN.
Тест на проникновение не должен использовать устройства за пределами их законных разрешений. Кроме того, если организация использует технологию удаленного доступа, не использующую туннелирование протоколов, само приложение и поддерживающая инфраструктура представляют собой единственные допустимые векторы атаки. Между ними нет ничего промежуточного для маршрутизации сетевого трафика — только для визуализации экранов и данных сеанса.

Предприятиям необходимо рассмотреть свои варианты и четко понимать, что входит в рамки теста на проникновение, а что выходит за его пределы. Хотя некоторые ресурсы остаются закрытыми для проверки на проникновение, вам все равно необходимо учитывать этот неизвестный/неопределенный риск в своем отчете.

политика управления рисками и операции по обеспечению безопасности.

Ключевой вывод

После того, как риски выявлены с помощью пентестирования и их природа хорошо понята, ваша организация может разработать планы смягчения последствий, такие как обучение, установка исправлений, удаление локальных административных прав, изменение конфигурации, усиление безопасности путей удаленного доступа и т. д.

Перекалибруйте свою безопасность с помощью BeyondTrust, чтобы Устраните сегодняшние угрозы

BeyondTrust предоставляет полный **Платформа управления привилегированным доступом** это помогает внедрить безопасную основу, необходимую организациям для обеспечения удаленной работы и цифровой трансформации, оставаясь при этом устойчивыми, адаптивными и защищенными..

Наши решения PAM предоставляют такие необходимые возможности, как**соблюдение минимальных привилегий, управление привилегированными учетными записями и учетными данными, а также безопасность удаленного доступа**, которые все чаще востребованы киберстраховщиками и являются неотъемлемой частью снижения киберрисков и киберответственности.

В приложении кОтчет Verizon о расследовании утечек данных за 2021 год (DBIR) Секретная служба США прокомментировала, как лучше защитить инфраструктуру:

«Положения и принципы безопасности, такие как правильная сегментация сети, предотвращение горизонтального перемещения, минимальные привилегии и принцип «никогда не доверяй, всегда проверяй», оказались убедительными индикаторами способности организации предотвращать несанкционированное присутствие в ее сетевой среде или восстанавливаться после нее. ».

Это все элементы управления безопасностью, которые BeyondTrust превосходно помогает обеспечить.

Решения BeyondTrust поддерживают умная, практичная реализация NIST (SP 800-207) нулевое доверие принципы. Наши решения гарантируют весь доступ соответствующий, адаптивный, детально контролируемый и ограниченный по сумме и продолжительности, а также документировано, независимо от того, как периметр был переопределен.

Платформа BeyondTrust состоит из четырех решений:

- Управление привилегированными паролями
- Безопасный удаленный доступ
- Управление привилегиями конечных точек
- Защита облачных привилегий

Вы можете развернуть эти решения отдельно или вместе как часть нашей интегрированной платформы, чтобы получить выгоду от синергии кибербезопасности и производительности труда.

Все решения BeyondTrust могут предоставляться локально, в облаке или посредством гибридного развертывания.

Платформа BeyondTrust PAM

Управление привилегированными паролями Решения обеспечивают автоматическое обнаружение и подключение всех привилегированных учетных записей, безопасный доступ к привилегированным учетным данным и секретам, а также аудит всех привилегированных действий.

Управление привилегиями конечных точек решения сочетают в себе управление привилегиями и контроль приложений для эффективного управления правами администратора на Windows, Mac, Unix, Linux и сетевых устройствах без снижения производительности.

Безопасный удаленный доступ Решения позволяют организациям применять минимальные привилегии и надежные средства контроля аудита для всего удаленного доступа, необходимого сотрудникам, поставщикам и службам поддержки.

Защита облачных привилегий Решения помогают организациям выявлять и снижать риски, связанные с разрешениями и правами на доступ к облаку в мультиоблачных средах.

НА ПОМЕЩЕНИИ ОБЛАКО ГИБРИДНЫЙ

За пределами понимания Открытие | Составление отчетов | Аналитика угроз | Разъемы | Центральная политика и управление

Если вы придерживаетесь превентивного подхода к управлению киберрисками, вам следует постоянно спрашивать:

Каков путь наименьшего сопротивления для субъекта угрозы и что можно сделать, чтобы он не стал вектором атаки?

В конечном счете, вы хотите, чтобы путь наименьшего сопротивления потенциального субъекта угрозы был другой компанией или целью. Однако в вашей среде вы должны постоянно переоценивать свои собственные пути наименьшего сопротивления и риск, который это представляет для вашей организации.

Эта оценка поможет обеспечить разумное развертывание технологий или корректировку настроек и инфраструктуры в соответствии с вашей склонностью к риску.

Дополнительные ресурсы

БЕЛАЯ БУМАГА	Руководство по управлению привилегиями мультиоблачной среды
БЕЛАЯ БУМАГА	Подход с нулевым доверием к безопасному доступу
РУКОВОДСТВО ПОКУПАТЕЛЯ	Контрольный список и руководство для покупателя по управлению привилегированным доступом (PAM)
РУКОВОДСТВО ПОКУПАТЕЛЯ	Контрольный список удаленной поддержки и руководство для покупателя

BeyondTrust

BeyondTrust — мировой лидер в области управления привилегированным доступом (PAM), который позволяет организациям защищать и управлять всей совокупностью своих привилегий. Наши интегрированные продукты и платформа предлагают самое передовое в отрасли решение PAM, позволяющее организациям быстро сократить поверхность атак в традиционных, облачных и гибридных средах.

Подход BeyondTrust Universal Privilege Management обеспечивает и защищает привилегии в отношении паролей, конечных точек и доступа, предоставляя организациям видимость и контроль, необходимые для снижения рисков, обеспечения соответствия требованиям и повышения операционной эффективности. Наши продукты обеспечивают необходимый уровень привилегий только на необходимое время, создавая для пользователей удобство работы и повышая производительность.

Благодаря наследию инноваций и твердой приверженности клиентам решения BeyondTrust легко развертываются, управляются и масштабируются по мере развития бизнеса. Нам доверяют 20 000 клиентов, включая 70 процентов компаний из списка Fortune 500, а также глобальная партнерская сеть.

Beyondtrust.com