SANS SECURITY AWARENESS

Руководство по обеспечению инфобезопасности: Как безопасно работать на дому

Резюме для руководства

Из-за коронавируса многие организации начинают переводить своих сотрудников на работу на дому. Это может стать проблемой, так как далеко не у всех имеются правила, технологии и программы обучения для обеспечения безопасности удаленных сотрудников. Кроме того, многие сотрудники могут быть незнакомы с самой идеей работы на дому или чувствовать себя при этом некомфортно. Цель данного руководства — дать вам возможность быстро научить таких людей обеспечивать максимальную безопасность, насколько это возможно. Если у вас возникли вопросы по использованию данного руководства, свяжитесь с нами по адресу support@sans.org.

Так как ваши сотрудники, скорее всего, испытывают огромный стресс, пытаясь приспособиться к переменам, а ваша организация, вероятно, ограничена во времени и ресурсах, данное стратегическое руководство сосредоточено на том, чтобы сделать обучение как можно более простым. Мы рекомендуем вам сосредоточиться только на наиболее важных рисках, которые окажут наибольшее влияние. Именно о них мы и расскажем ниже. Расценивайте это как отправную точку. Если есть дополнительные риски или темы, которые вы хотите добавить, обязательно сделайте это. Необходимо понимать: чем больше моделей поведения, процедур или технологий вы потребуете от своих сотрудников, тем ниже шансы их полного внедрения.

Как использовать это руководство

Мы рекомендуем начать с прочтения материала, представленного в данном руководстве, и просмотреть ссылки на различные материалы, чтобы получить представление о том, что есть в наличии. Вы увидите, что для каждого риска мы предоставляем разные материалы, которые можно задействовать для обучения в рамках организации. Это позволит вам выбрать оптимальные методы под собственные потребности и культуру. Закончив чтение этого руководства, ознакомьтесь также с сопутствующими документами: «Работа на дому: донесение информации (шаблон)» и «Информационный обзор» в этом же комплекте. Они позволят лучше понять, чего требуется достичь. После ознакомления с документацией необходимо согласовать действия с двумя ключевыми группами.

1. **Отдел безопасности**: согласуйте свои действия с отделом безопасности для лучшего понимания того, какими основными рисками вам предстоит управлять. В данном руководстве мы определили, по нашему мнению, основные и наиболее распространенные риски для сотрудников, работающих на дому, но ваши риски могут отличаться. Внимание! Распространенная ошибка, которую допускают отделы безопасности, — это попытки управлять всеми рисками, что приводит к слишком большому количеству правил и требований. Постарайтесь ограничить количество

рисков, с которыми будете иметь дело. После того как вы определили эти риски и установили для них приоритеты, подтвердите модели поведения для управления этими рисками. Как уже упоминалось, если у вашей организации нет на это времени или ресурсов, то воспользуйтесь средствами, описанными ниже.

2. **Отдел коммуникаций**: определив основные риски для сотрудников и ключевые модели поведения для управления этими рисками, скооперируйтесь с отделом коммуникаций для обучения сотрудников выработанным моделям поведения. Самые эффективные программы повышения осведомленности в области безопасности прочно связаны с отделом коммуникаций. По возможности подумайте, можете ли вы внедрить кого-нибудь из этого отдела в отдел безопасности. При общении с сотрудниками эффективным средством их привлечения может стать акцент на том, что обучение не только обеспечит безопасность в работе, но и позволит создать дом с высоким уровнем кибербезопасности, защитив тем самым их самих и их близких.

Вага конечная задача при работе с этими двумя группами — как максимально упростить вопрос безопасности для сотрудников и мотивировать их. Это два ключевых элемента для изменений в поведении. Мы предлагаем вам также создать консультативный совет из сотрудников, занимающих ключевые должности, чья обратная связь и вклад необходимы для продвижения программы. Помимо отдела безопасности и отдела коммуникаций вам также, вероятно, имеет смысл рассмотреть сотрудничество с отделом кадров и юридическим отделом.

Загружаемый цифровой пакет MGT433

SANS Institute проводит двухдневные курсы обучения MGT433: Как создать, поддерживать и оценивать высокоэффективную программу повышения осведомленности в области безопасности (How to Build, Maintain and Measure a High-Impact Security Awareness Program). Этот интенсивный курс знакомит вас со всеми теоретическими выкладками, навыками, концепциями и ресурсами для создания высокоэффективной программы повышения осведомленности, позволяющей эффективно управлять человеческими рисками и определять их. В рамках данного руководства мы предоставляем бесплатный доступ к загружаемому цифровому пакету курса с шаблонами и ресурсами планирования. Хотя вполне вероятно, что эти материалы выходят за рамки потребностей данной инициативы, они могут оказаться ценными для более крупных организаций или более сложных операций.

Реагирование на вопросы сотрудников

В дополнение к общению с сотрудниками и их обучению мы настоятельно рекомендуем использовать технологии или форумы, где можно ответить на вопросы, причем желательно в режиме реального времени. Это может быть специальный адрес

электронной почты, канал чата Skype или Slack либо какой-то сетевой форум, например в Yammer. Другой вариант — проводить веб-трансляцию по вопросам безопасности несколько раз в неделю. Это позволит всем сотрудникам выбрать подходящее время, присутствовать мероприятии в прямом эфире и, возможно, даже задавать вопросы. Цель здесь в том, чтобы сделать безопасность как можно более доступной и дать людям ответы на их вопросы. Это великолепная возможность вовлечь ваш персонал, продемонстрировать, что безопасность не так сложна, как кажется, и извлечь из обстоятельств максимум пользы. Учтите, что для достижения эффективности нужно выделить ресурс для модерации любых каналов безопасности и активного реагирования на запросы.

Риски и учебные материалы

Мы определили три основных риска, которыми вам необходимо управлять в связи с удаленными сотрудниками. Это отправная точка, и, вероятнее всего, именно они будут иметь для вас наибольшую ценность. Каждый приведенный ниже риск имеет ссылки на многочисленные ресурсы, помогающие общению и проведению обучения по данной теме. Мы предоставляем множество коммуникационных материалов, чтобы вы могли выбрать те, которые окажут наибольшее влияние на культуру в вашей организации. Кроме того, почти все материалы предоставляются на нескольких языках. Если массив информации кажется чрезмерным, а ваше время крайне ограничено, то мы рекомендуем вам просто рассмотреть два приведенных ниже материала.

1. Информационный бюллетень «Как безопасно работать на дому» (входит в ваш комплект средств).
2. Видео «Creating a Cybersecure Home video (Кибербезопасность вашего дома)» (на английском языке), также доступное на других языках здесь.

Социальный инжиниринг

Один из самых больших рисков, с которым столкнутся сотрудники при удаленной работе, особенно в это время коренных изменений и чрезвычайных ситуаций, — это информационно-психологические атаки (социальный инжиниринг). Применяя социальный инжиниринг, которой взломщики обманывают своих жертв, чтобы те совершили ошибку, а это легче сделать во время перемен и замешательства. Ключевой момент здесь — объяснить сотрудникам, что такое социальный инжиниринг, как распознать самые распространенные признаки подобной атаки и что делать при ее обнаружении. Обязательно сконцентрируйтесь не только на фишинговых атаках по электронной почте, но и на других методах, включая телефонные звонки, текстовые сообщения, социальные сети или фальшивые новости. Материалы, необходимые для

обучения данной теме и ее закрепления, можно найти в нашей папке «Social Engineering Support Materials (Материалы в помощь по теме социального инжиниринга)». Кроме того, вот еще два видео по инфобезопасности от SANS. Они доступны по ссылке и также предоставлены на нескольких языках.

- Видео «Social Engineering (Социальный инжиниринг)» (на английском языке), также доступное на других языках здесь.
- Видео «Phishing (Фишинг)» (на английском языке), также доступное на других языках здесь.

Надежные пароли

Как отмечается в ежегодном отчете DBIR от Verizon, слабые пароли по-прежнему являются одним из основных факторов, способствующих взломам в глобальном масштабе. Ниже приведены четыре ключевые модели поведения, помогающие управлять этим риском. Материалы, необходимые для обучения данной теме и ее закрепления, и эти модели поведения можно найти в нашей папке «Passwords (Пароли)».

- Кодовые фразы (примечание: такие темы, как сложность паролей иистекшие пароли, устарели).
- Уникальные пароли для всех учетных записей
- Менеджеры паролей
- Многофакторная аутентификация. (часто называется двухфакторной аутентификацией или двухшаговой проверкой)

Обновления систем

Третий риск заключается в том, что ваши сотрудники должны использовать при работе последние версии операционной системы и приложений, в том числе мобильных. Сотрудникам, использующим личные устройства, придется включить автоматическое обновление. Материалы, необходимые для обучения данной теме и ее закрепления, можно найти в папках «Malware (Вредоносное программное обеспечение)» или«Creating a Cybersecure Home (Кибербезопасность вашего дома)».

Дополнительные темы для размышления

- **Wi-Fi**: защита вашей точки доступа Wi-Fi. Данная тема рассматривается в материалах «Creating a Cybersecure Home (Кибербезопасность вашего дома)». Также обратите внимание на видео «Creating a Cybersecure Home (Кибербезопасность вашего дома)» (на английском языке), также доступное на других языках здесь.

- **VPN**: что такое VPN и почему его нужно использовать. Мы рекомендуем информационные письма OUCH, в которых говорится о VPN.

- **Удаленная работа**: Предназначено для тех, кто работает удаленно, но НЕ дома, например в кафе, терминале аэропорта или гостинице. Используйте наше обучающее видео «Working Remotely (Удаленная работа)» (на английском языке) , также доступное на других языках здесь.

- **Дети и гости**: Чтобы закрепить мысль о том, что члены семьи и гости не должны иметь доступ к устройствам, связанным с работой, используйте обучающее видео «Working Remotely (Удаленная работа)» (на английском языке), также доступное на других языках здесь.

- **Обнаружение и реагирование**: Вы хотите, чтобы сотрудники сообщали о возможных инцидентах при работе на дому? Если да, то что и когда они должны сообщать? Это описывается в наших материалах по теме «Взлом».

Информационные письма OUCH

Кроме того, воспользуйтесь для вашей программы находящимися в открытом доступе информационными письмами OUCH, переведенными более чем на 20 языков. Ниже перечислены информационные письма OUCH, которые, по нашему мнению, лучше всего помогут вам в инициативе «Как безопасно работать на дому». Вы сможете найти все информационные письма в сетевом архиве информационных писем OUCH по инфобезопасности (OUCH Security Awareness Newsletter Archives).

ОБЗОР

Four Steps to Staying Secure (Четыре ступени безопасности)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Кибербезопасность вашего дома)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

СОЦИАЛЬНЫЙ ИНЖИНИРИНГ

Social Engineering (Социальный инжиниринг)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (Текстовые сообщения и SMS-фишинг)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (Персонализированное мошенничество)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (Имитирование начальства)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (Телефонные атаки и мошенничество)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (Осторожно, фишинг!)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Мошенничество в социальных сетях)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

ПАРОЛИ

Making Passwords Simple (Просто о паролях)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (Защита входа (двухфакторная аутентификация))
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

ДОПОЛНИТЕЛЬНО

Yes, You Are a Target (Да, вы на прицеле)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (Умные домашние устройства)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Советы

Советы и рекомендации, которыми можно поделиться в легко усваиваемом формате.

- Самые эффективные меры для безопасности беспроводной сети дома — это сменить стандартный пароль администратора на свой, применить шифрование WPA2 и использовать надежный пароль для беспроводной сети.
- Выясните, какие именно устройства подключены к вашей домашней сети, в том числе радионяни, игровые консоли, телевизоры, бытовые приборы и даже автомобиль. Убедитесь, что все эти устройства защищены надежным паролем и (или) что на них установлена последняя версия операционной системы.
- Для эффективной защиты вашего компьютера дома обязательно следите, чтобы операционная система и приложения были обновлены до последней версии с установкой всех нужных исправлений. По возможности используйте функцию автоматического обновления.
- В конечном счете ваша лучшая защита — это здравый смысл. Если письмо, сообщение или звонок выглядят странно, подозрительно или слишком заманчиво, — вероятно, это атака.
- Используйте уникальные пароли на каждой из учетных записей. Не можете запомнить все свои пароли и кодовые фразы? Для их безопасного хранения можно использовать менеджер паролей.
- Один из лучших способов обеспечить безопасность любой учетной записи —

двухшаговая проверка. Она заключается в том, что вам требуется не только пароль, но и код, который отправляется на ваше мобильное устройства или генерируется им. Среди сервисов, поддерживающих двухшаговую проверку, Gmail, Dropbox и Twitter.

- Фишинг — это попытки злоумышленника обманом заставить вас нажать на вредоносную ссылку или открыть вложение в электронном письме. С подозрением относитесь к любому электронному письму или текстовому сообщению, в которых создается ощущение срочности, имеются орфографические ошибки или обращение типа «Дорогой клиент!».

Показатели

С показателями поведения в данном случае трудно, так как определить, как люди ведут себя дома, гораздо сложнее. Кроме того, некоторые действия не связаны конкретно с работой (например, защита устройства Wi-Fi). Однако можно оценить такой показатель, как вовлеченность. Мы обнаружили, что такие личные или эмоциональные темы могут очень захватывать людей, вызывая гораздо больший интерес, чем другие темы. Таким образом, подобные показатели могут иметь ценность.

- **Взаимодействие**: Насколько часто люди задают вопросы, высказывают идеи или просят о помощи на любом из каналов или форумов по вопросам безопасности, которые вы организовали?
- **Моделирование**: моделируйте ситуации, связанные с социальным инжинирингом, например атаки на основе фишинга, текстовых сообщений или телефонных звонков.

Чтобы посмотреть более полный список показателей, загрузите интерактивную «Таблицу показателей осведомленности в области безопасности» (Security Awareness Metrics Matrix) из загружаемого цифрового пакета MGT433.

Лицензия

Автор комплекта средств

Ланс Спицнер имеет более 20 лет опыта в сфере безопасности (исследования киберугроз, архитектура безопасности, осведомленность и обучение в области безопасности). Он был одним из первопроходцев в сфере заманивания хакеров и киберразведки благодаря созданию «медовых сетей» и основанию Honeynet Project. Будучи инструктором SANS, он разработал курсы MGT433: Security Awareness (Осведомленность в области безопасности) и MGT521: Security Culture (Культура безопасности). Кроме того, Ланс издал три книги по теме инфобезопасности, проводил консультации в более чем 25 странах и помог более 350 организациям создать программы повышения уровня осведомленности и культуры в области безопасности для управления человеческими рисками. Ланс часто дает презентации, пишет в Twitter (@lspitzner) и работает над многочисленными проектами по общественной безопасности. Прежде чем заняться информационной безопасностью, Ланс Спицнер прослужил офицером бронетанковых войск в силах быстрого реагирования армии США и получил степень магистра бизнеса в Иллинойсском университете.

О SANS Institute

SANS Institute был основан в 1989 году как кооперативная научно-исследовательская и образовательная организация. SANS — самый надежный и крупный поставщик услуг по обучению и сертификации в области кибербезопасности для профессионалов в правительственных органах и коммерческих учреждениях по всему миру. Известные инструкторы SANS проводят более 60 различных курсов в рамках более 200 мероприятий по обучению кибербезопасности, а также онлайн. GIAC, филиал SANS

Institute, подтверждает квалификацию специалиста-практика при помощи более 35 видов технической сертификации в сфере кибербезопасности. Технологический институт SANS (SANS Technology Institute), регионально аккредитованная независимая дочерняя компания, предлагает степень магистра по кибербезопасности. SANS предлагает множество бесплатных ресурсов сообществу инфобезопасности, включая консенсусные проекты, исследовательские отчеты и информационные бюллетени, а также управляет Internet Storm Center, системой раннего предупреждения в Интернете. Основу SANS составляют множество специалистов-практиков, представляющих различные мировые организации от корпораций до университетов, работающих вместе для того, чтобы помощь всему сообществу инфобезопасности. (https://www.sans.org)