7 ЛУЧШИХ ПРАКТИК КИБЕРБЕЗОПАСНОСТИ

2N
An Axis company

РЕГУЛЯРНО ОБНОВЛЯЙТЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Регулярное обновление версий программного обеспечения является обязательным условием, если вы хотите минимизировать возможные риски, связанные с кибер-безопасностью. Когда производитель выявляет потенциальный сбой в работе программного обеспечения, он исправляет его в следующей версии программного обеспечения. **Установка обновлений программного обеспечения даст вам гарантию того, что вы исправите уязвимости вашего ПО вместе со всеми выявленными сбоями.**

2N
An Axis company

ИСПОЛЬЗУЙТЕ СИЛЬНЫЕ ПАРОЛИ

Самое малое что вы можете сделать как пользователь, **это создать сложный пароль, который будет сложно взломать.** Идеальный пароль должен состоять по крайней мере с шести знаков. Он должен включать в себя числа, буквы и символы. Вполне очевидно, что это далеко не самая лучшая стратегия использовать пароли, которые можно легко угадать, такие как дата вашего рождения или название вашего родного города. Если у вас получиться создать сильный пароль, это замечательно. Однако **не стоит обмениваться вашими личными данными с другими пользователями.** Даже если вы следуете этим правилам, было бы неплохо, если бы вы время от времени меняли свой пароль.

2N
An Axis company

РАЗНЫЕ АККАУНТЫ ДЛЯ РАЗНЫХ ЗАДАЧ

Очень важно иметь **несколько аккаунтов с разными привилегиями.** Пользователю будет разрешено вносить только те изменения, которые имеют непосредственное отношение к задачам, связанным с его работой. Еще раз стоит отметить, даже для этих типов аккаунтов не стоит делится своим паролем с другими людьми. Таким образом вы минимизируете возможность утечки ваших конфиденциальных данных в пределах компании.

2N
An Axis company

МИНИМИЗИРУЙТЕ НЕЗАЩИЩЕННОСТЬ ПОДКЛЮЧЕНИЯ К ИНТЕРНЕТУ

Чтобы избежать вредоносных программ, используйте брандмауер, созданный на основе маршрутизаторов, который обнаруживает подозрительный трафик, прежде чем он попадет в сеть. Конечно, вариант с отключением от сети интернет полностью исключается. Однако очень важно проявить внимательность и **защитить сеть с сильным паролем.** Хакеры постоянно сканируют Интернет, чтобы обнаружить технику, которая подвергается риску. Если вы хотите знать, какие места открыты для сети с устройства, которое вы используете, вы можете посетить www.shodan.io, чтобы получить больше информации. Чем больше устройств вы защитите от сетевых угроз, тем меньшему риску вы подвергаетесь. Обращаем ваше внимание, **что вам необходимо будет активировать только ключевые функции продуктов.**

2N
An Axis company

ЗАЩИТИТЕ СЕТЬ

a) Создайте **независимую сеть,** которая предназначена исключительно для устройств с незащищенной информацией. Сделайте так, чтобы было практически невозможно попасть в сеть имея отдельные переключатели.

b) Используйте **виртуальный LAN (VLAN).** VLAN содержит изолированные сети в пределах дата центра, и каждая сеть является отдельным широковещательным доменом.

c) Актуально также обеспечить безопасность сети через **протокол IEEE 802.1X.** Он не дает возможность неавторизированным устройствам получить доступ к локальной сети.

d) Убедитесь, что производители устройств или программного обеспечения, которые вы используете, задействуют такие протоколы как **HTTPS, TLS, SIPS or SRTP,** которые включены по умолчанию. Они также предотвращают тип хакерских атак под названием «Человек посредине».

2N
An Axis company

ВЫБЕРИТЕ ПОДХОДЯЩЕГО ПРОВАЙДЕРА ДИСТАНЦИОННОГО УПРАВЛЕНИЯ

Очень удобно **управлять всеми локациями установки с помощью одного аккаунта.** Локация установки не имеет значения, вы сможете получить к ней доступ удаленно, не выходя с вашего офиса. Это может показаться рискованным, учитывая все вышеперечисленные угрозы для устройств в сети Интернет. Ищите провайдера дистанционного управления, чей сервис работает на безопасном облаке. В этом случае, **вам больше не нужно будет иметь дело с брандмауерами, созданными на основе маршрутизатора или туннелизации.** Облачный сервис **самостоятельно установит шифрованную связь.**

2N
An Axis company

ОБЕСПЕЧЬТЕ БЕЗОПАСНОСТЬ ЭКОСИСТЕМЫ IOT

Создайте **отдельную сеть для устройств IoT,** выберите **сильный пароль для роутера,** чтобы защитить сеть, **никогда не устанавливайте какую-либо электротехнику не проверив ее производителя,** не активируйте ненужные функции на устройствах и регулярно обновляйте программное и **аппаратное обеспечение.**

2N
An Axis company