Компания ITC Holdings сосредоточилась на защите своих материальных и электронных активов

Энди Хильверда

Вандализм, воровство, возможность саботажа или террористических актов вынудила предприятия энергетической отрасли искать жизнеспособные решения для обеспечения безопасности. В этом поиске они столкнулись с уникальными проблемами, связанными со структурой отрасли. Компании должны обезопасить свои объекты, а также защитить физические и электронные активы, управляя доступом на объекты штат за штатом по географически разобщенным регионам.

Компания ITC Holdings, Inc. предприняла экстраординарные шаги для защиты физических и электронных активов, чтобы сохранить целостность своей массовой электросистемы. Обосновавшаяся в Нови, штат Мичиган, компания ITC построила, обслуживает и использует 15,000 миль воздушных и подземных линий электропередачи, которые доставляют электроэнергию более чем 13 миллионам потребителей, охватывая территорию площадью около 80000 квадратных миль.

Ощутив серьезный удар по местной и национальной экономике и жизням людей, когда отключилось электроснабжение, компания ITC приоритетной задачей сделала защиту сети электропередачи и эффективную, надежную поставку энергии потребителям. ITC компания намерена внедрить на местах высокоэффективные процессы и процедуры, которые соответствуют правительственным стандартам безопасности и даже превышают их.

Роберт Бликенсдорф, менеджер по безопасности компании ITC, несет ответственность за управление проектами во всем, что касается установки, обслуживания и использования физической безопасности на объектах компании ITC. Он служит посредником между компанией ITC и местными правоохранительными органами и другими организациями, обеспечивающими безопасность в отрасли.

Бликенсдорф рассказывает: “Руководство корпорации ITC понимает важность защиты наших физических и электронных активов, и с энтузиазмом поддерживает наши инициативы в области обеспечения безопасности. Столкнувшись с огромным разнообразием вариантов и цен, компания ITC разработала основанную на рисках методологию для достижения уравновешенного подхода к осуществлению целей обеспечения безопасности. Компании ITC нужно было определить тип физической защиты, который лучше всего служил бы на каждом отдельном участке, установить и интегрировать необходимые защитные устройства, а затем поддерживать и отслеживать эффективность системы."

В связи с возникшей угрозой вандализма и краж из-за высокой стоимости меди и других металлов на открытом рынке, компания ITC приняла меры для предотвращения доступа на свои объекты лиц, намеревающихся украсть металл и, по ходу дела, нанести повреждения, которые нарушили бы надежность системы и подвергли бы опасности сотрудников и подрядчиков. Из-за изолированности повышенной уязвимостью отличаются удаленные объекты компании. Чтобы решить эти проблемы, на таких объектах устанавливаются устройства безопасности, предотвращающие вандализм или кражи. Бликенсдорф рассказал: "Мы не хотим давать каким бы то ни было лицам или организациям возможность саботировать систему, так как вмешательство влечет серьезные последствия.”

Главное управление компании ITC (фото предоставлено Робертом Бликенсдорфом из ITC)

Камера реального времени на столбе за ограждающим периметром (фото предоставлено Робертом Бликенсдорфом из ITC)

Бликенсдорф наблюдает за работой Центра управления службы безопасности компании ITC, который работает 24 часа в сутки, 7 дней в неделю. Центр управления службой безопасности следит за камерами реального времени и системой сигнализации всех их объектов. Система охранной сигнализации с видеоподтверждением стала более практичной, так как стоимость системы видеонаблюдения CCTV (closed circuit television cameras – замкнутая система видеонаблюдения) снизилась, делая ее доступным способом для повышения безопасности.

На сегодняшний день, компания ITC установила не меньше 300 камер наблюдения, параллельно интегрированных в охранную сигнализацию на 30 своих объектах. Благодаря усовершенствованной системе безопасности на местах, персонал центра управления службы безопасности может быстро определить, когда проникновение не представляет угрозы, а когда более серьезно.

Проект физической защиты компании ITC охватывает главное управление, подстанции и склады. В дополнение к камерам реального времени, заграждающий периметр с отслеживанием вторжения, фотодатчики, устройства ИК освещения и другое оборудование для физической защиты в стратегических точках. Они также внедрили онлайн систему карт доступа, установленную по всем объектам. При любом неавторизированном доступе или другой тревоге, информация об этом быстро поступает в центр управления службы безопасности для принятия мер.

Федеральная комиссия по управлению энергетикой (FERC) и Северо-американская

Навесной замок CyberLock на шкафе ITU (фото предоставлено Робертом Бликенсдорфом из ITC)

корпорация надежности электроэнергетики (NERC) установили обязательные стандарты обеспечения безопасности, чтобы предотвратить электронные и физические атаки, которые могут нанести ущерб энергетике, представляющей критическое звено национальной инфраструктуры.

В январе 2008 с целью защиты физической безопасности критических электронных активов были одобрены Стандарты надежности защиты критических звеньев инфраструктуры (CIP). Стандарт CIP 006-1 гласит: “необходимо ответственное лицо для создания и поддержания плана физической безопасности, который гарантирует, что все электронные активы защищены периметром электронной безопасности, а также входят в установленный периметр физической защиты. План обеспечения физической безопасности ... должен предусматривать процессы идентификации, контроля и отслеживания всех точек доступа и запросов авторизации. Стандарты надежности также требуют, в каждом случае физического доступа должна производиться регистрация, а регистрационная информация должна быть достаточной для однозначной идентификации личности."[1]

При разработке стратегии приведения в соответствие требованиям стандартов надежности CIP, компания ITC столкнулась с логистическими проблемами.

Когда они взялись за решение этого вопроса, то искали надежную систему контроля доступа, обладающую необходимой им гибкостью. Важнее то, что им нужна была система, способная обеспечить контроль ключей и ведение контрольных записей на удаленных объектах и не требующая подведения электропитания к замкам.

Бликенсдорф комментирует: "Нам нужна была система, способная исключить риски, связанные с изготовлением дубликатов ключей и помочь соблюдать требования CIP в отношении отслеживания подрядчиков и сотрудников, имеющих доступ в места, где имеются критические электронные активы.” Они искали продукт, который можно интегрировать со сложными средствами обеспечения безопасности и системами, уже установленными на местах.

После всестороннего исследования, организация выбрала установку системы CyberLock и приступила к интеграции электронной запирающей системы в свои уже существующие системы. Компания ITC обратилась за помощью в компанию Janna Access LLC, занимающуюся интегрированием систем контроля доступа, которая обосновалась в Колмабия-Стейшн, штат Огайо. “Сотрудники компании Janna Access выехали на место и очень тесно сотрудничали с нашим IT персоналом. Компания Janna предоставила нам необходимую для интеграции системы IT поддержку и выполнила необходимое для работы с системой обучение нашего персонала." – рассказал Бликенсдорф.

Компания ITC заменила цилиндры в механических замках электронными цилиндрами.

Замок CyberLock, установленный на коробку Net Shelter (фото предоставлено Робертом Бликенсдорфом из ITC)

Они установили электронные замки на свои удаленные терминалы, шкафы NetShelter и двери помещений с контрольно-измерительными приборами. Электронные навесные замки защищают их коробки TMedic и ворота ограждающего периметра. “Материальные и электронные активы, которые мы защищаем с помощью электронных замков, являются критическими участками в соответствии со стандартами надежности CIP.” – рассказал Бликенсдорф.

Компания ITC выдала электронные ключи своим подрядчикам и полевым служащим, которым необходим доступ на подстанции и другие уязвимые зоны. Компания ITC для работ в полевых условиях преимущественно использует наемную рабочую силу. Эти рабочие обычно заняты полный рабочий день на проектах компании ITC и выполняют обслуживание сети электропередач. Им необходим доступ на подстанции, чтобы выполнять свою работу. Компания ITC программирует электронный ключ каждого уполномоченного лица правами доступа, необходимыми для выполнения определенных работ.

Использование электронных ключей исключает проблемы, с которыми компания ITC сталкивалась в прошлом, когда использовала механические ключи. Ключи копировали и передавали, ключи оставались у бывших сотрудников, ключи терялись и не учитывались. “С новым ограничивающим ключом на местах, мы получили отчетность и электронные записи о том, где использовался ключ, как его использовался и кем." - сообщил Бликенсдорф. В каждом ключе установлен срок действия для снижения рисков, связанных с утерей ключей. При пропаже ключа, компания ITC может быстро деактивировать его или положиться на автоматическое истечение срока действия ключа.

“Каждое предприятие в отрасли стремится к достижению соответствия нормам CIP.” – утверждает Бликенсдорф. Он добавил: “Электронная запирающая система помогает нам соответствовать стандартам CIP благодаря отслеживанию личностей, имеющих доступ к зонам, которые содержат критические электронные активы.” Где бы ни был расположен электронный замок, в любой момент можно считать с него информацию и определить, кто в последнее время получал доступ в эту определенную зону. Ключ любого уполномоченного пользователя запрограммирован на доступ к отобранным замкам в определенных зонах и только в отведенное время в течение дня. Электронные замки и ключи ведут учет открываний и попыток неавторизированного доступа в зоны, которые защищают электронные данные и расположенное в них оборудование.

“Электронная запирающая система осуществляет двухвекторный подход к контролю физического доступа к нашим электронным активам. Во-первых, мы можем контролировать, кому мы выдали ключ и как этот ключ будет использоваться этим лицом. Во-вторых, мы может отслеживать деятельность этого лица на разных объектах" – подытожил Бликенсдорф.

Компания ITC стремится ввести на местах лучшие меры безопасности для защиты надежности их сети, которая продолжает расти. Благодаря кооперации с квалифицированным интегратором систем контроля доступа и использованию преимуществ современных достижений технологий обеспечения безопасности, они внедрили систему обеспечения безопасности, которая продолжит обеспечивать необходимый им уровень физической безопасности и подотчетности. С ужесточением правительственных стандартов и появлением новых угроз безопасности, компания ITC заняла сильную позицию реагировать быстро и решительно.

Об авторе:

Энди Хильверда является вице президентом компании Videx, Inc., компании, которая разработала и производит средства обеспечения безопасности и электронную запирающую систему CyberLock

[1]www.NERC.com