Анна Табульда, Светлана Чернущенко

Чек-лист по кибербезопасности для специалистов по автоматизации

Итак, у нас есть промышленное предприятие, руководство которого делает всё возможное, чтобы вести бизнес в сложных экономических условиях. Главные вопросы ежедневной повестки связаны с движением денежных средств, ростом продаж, качеством продукции и никак не затрагивают кибербезопасность.

Конечно, все мы следим за новостными лентами и постоянно слышим слова «кибер», «кибератака» и «информационная безопасность». И хотя у вас, скорее всего, есть общее понимание того, что эти слова означают, на самом деле они не сильно интересуют вас, ведь «инициаторами всех произошедших кибератак были террористические организации», не так ли? А ваше предприятие относится к малому или среднему бизнесу, и «никто по-настоящему не заинтересован в бизнесе такого масштаба», так что на самом деле «вся эта кибербезопасность не касается нас», верно?

Кибератаки осуществляются разными людьми по разным причинам. В любом случае, будь то организованные киберпреступники или неутомимый хакер-любитель, ваш бизнес находится под угрозой.

Угрозы безопасности АСУ ТП

Есть целый ряд статистических исследований, которые показывают, что киберпреступность в сфере систем автоматизации сегодня находится на подъёме [1–4]. Согласно данным

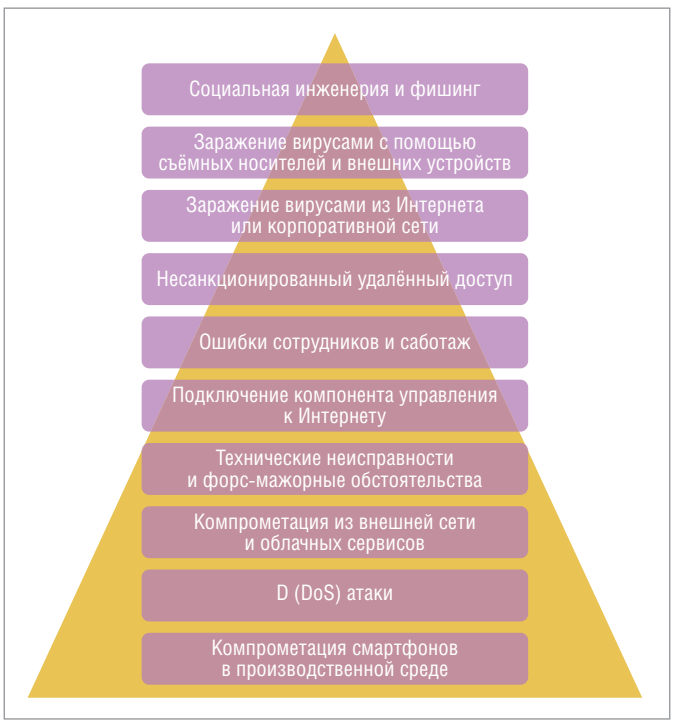

Рис. 1. Топ-10 угроз информационной безопасности промышленных систем автоматизации за 2016 год

Таблица 1

Примеры реализации угроз информационной безопасности промышленных систем автоматизации

Действия, которые привели к реализации угрозы	Реализованная угроза
Невнимательность, игнорирование предупредительных сообщений от программ [6].	**«Социальная инженерия и фишинг» и «Ошибки сотрудников».** Атака на энергетическую компанию была осуществлена через отправку фишингового сообщения по электронной почте на адрес жертвы, которое включало в качестве вложения XLS-файл. Данный файл содержал вредоносный макрос, который, используя методы социальной инженерии, обманул жертву, провоцируя её на игнорирование сообщения безопасности Microsoft Office Security Warning. Результат: отключение электроэнергии прямым воздействием вредоносной программы или же путём предоставления удалённого доступа злоумышленникам, которые выполнили необходимые операции своими руками.
Использование неучтённого съёмного носителя, отсутствие проверки носителя на вирусы перед использованием, отсутствие обновлений ОС и другого ПО [7].	**«Заражение вирусами с помощью съёмных носителей и внешних устройств».** По меньшей мере на 18 мобильных носителях данных (в основном на USB-носителях) и офисных компьютерах АЭС обнаружено вредоносное ПО, которое способно отключать ряд служебных сервисов ОС Windows и всячески вредить нормальному функционированию рабочих станций.
Создание в целях удобства несанкционированного канала передачи информации, выходящего за пределы контролируемой зоны [8].	**«Заражение вирусами из Интернета или корпоративной сети».** Использование модема для организации удалённого подключения вендора к оборудованию, при этом аутентификация проводилась с использованием крайне простых логина и пароля. Результат: заражение вредоносным программным обеспечением из-за использования непредусмотреннго беспроводного маршрутизатора с прямым подключением к сети управления.
Создание в целях удобства несанкционированного беспроводного канала передачи информации, выходящего за пределы контролируемой зоны [9].	**Действия, которые могли привести к реализации угрозы «Несанкционированный удалённый доступ».** Инженер АСУ ТП, чтобы не ходить по несколько раз в день по дамбе и не отслеживать работоспособность всех устройств (особенно в плохую погоду), поставил в центре дамбы точку доступа, завёл на неё исполнительные устройства и снимал с них информацию, не выходя из диспетчерской.

немецкого Федерального управления по информационной безопасности (BSI), топ-10 угроз информационной безопасности промышленных систем автоматизации за 2016 год [5] выглядит так, как показано на рис. 1.

В таблице 1 приведены некоторые примеры реализации угроз, включая действия, которые могут привести к ним.

С наличием бизнес-конкуренции, современных программно-технических средств и «моды» на кибератаки шансы быть атакованным с каждым днём возрастают и затраты на восстановление системы тоже. Таким образом, проблема безопасности перерастает в бизнес-проблему, которая так же нуждается в управлении, как и любая другая угроза для вашего бизнеса.

Да-да, скажете вы, всё это ясно, но где найти средства? В текущей экономической ситуации в полный рост встают совершенно иные проблемы: рост кредитных ставок, изменение курса валюты, сокращение штата, кассовый разрыв и т.д. Но большое складывается из меньшего, и даже ничего не зная о кибербезопасности и не делая материальных затрат, но будучи специалистом по автоматизации, при помощи данной статьи вы сможете заложить первый камень в фундамент защиты вашей АСУ ТП.

Мы составили чек-лист для специалистов по промышленным системам автоматизации, который основан на произошедших инцидентах и лучших практиках защиты информации в АСУ ТП и призван помочь вам не стать мишенью кибератаки.

Чек-лист по кибербезопасности

Съёмные носители

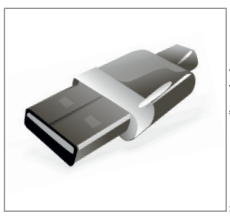
Иллюстрация с сайта pixabay.com

- Используйте только учтённые носители информации (хорошо, если за вас это делает программное средство защиты, если же оно не установлено, регистрируйте носитель в журнале, присваивайте учётный номер). Используйте учтённый носитель только в рабочих целях и только на рабочей станции. Если есть возможность, лучше, чтобы учтённый носитель был персонально вашим.
- Храните учтённые носители в безопасном месте (например, в запираемом шкафу), не берите учтённые носители домой, не давайте для личных целей сотрудникам и сами в личных целях не используйте.
- Проверяйте учтённые съёмные носители перед использованием в АСУ ТП на вирусы.
- Не подключайте сотовые модемы к рабочим станциям.

Сетевое оборудование


Иллюстрация с сайта pixabay.com

- Проверьте, чтобы отсутствовали ресурсы, доступные одновременно из сети АСУ ТП и сети корпоративной ЛВС.
- Для входа в интерфейс управления сетевого оборудования должны использоваться отдельные учётные записи.
- Храните журналы событий сетевого оборудования не менее одного года.
- Отключите неиспользуемые порты и разместите сетевое оборудование в запираемом шкафу.
- Храните резервную копию конфигурации сетевого оборудования и эталонную копию встроенного ПО.

Управление доступом

Иллюстрация с сайта pixabay.com

- Для доступа в операционную систему, а также в привилегированный конфигурационный режим должны быть созданы отдельные учётные записи, недоступные операторам.
- Не сообщайте данные о своих учётных записях (логин, пароль) никому (даже сотруднику, который представился новым администратором).
- Привилегии доступа должны быть назначены строго для выполнения служебных обязанностей и не сверх того.
- Используйте только свою учётную запись, после окончания работы завершите сеанс своей учётной записи. Если смена учётной записи не предусмотрена технологическим процессом, необходимо ведение журнала для отслеживания процесса смены пользователей. Помните, что это поможет при расследовании инцидентов и обезопасит вас.

Физический доступ

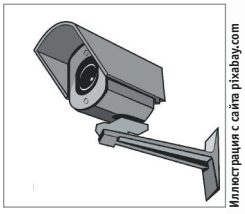
Иллюстрация с сайта pixabay.com

- Ограничьте доступ ко всем системным блокам рабочих станций АСУ ТП путём их помещения в железные ящики с замками.
- Пока железные ящики не установлены, заблокируйте порты и интерфейсы, которые вы не используете в рабочем процессе (если не на программно-аппаратном уровне, то с помощью воска, блокираторов, опечатывающих устройств).
- Проверьте наличие замков на серверных стойках и шкафах автоматики.
- И да: несколько недорогих IP-камер на наиболее критичных узлах АСУ ТП очень дисциплинируют операторов.

Документирование

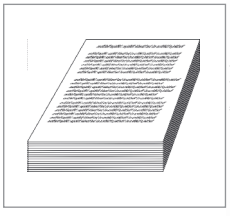
Иллюстрация с сайта pixabay.com

- Определите лица, ответственные за обеспечение защиты информации в АСУ ТП.
- Составьте и поддерживайте в актуальном состоянии список всех технических средств АСУ ТП, найдите по возможности эксплуатационную документацию на каждую систему.
- Разработайте организационно-распорядительные документы (в виде отдельных инструкций или в рамках общей политики обеспечения ИБ), определяющие правила и процедуры по защите информации в АСУ ТП, в которых будут введены ограничения на несанкционированные действия персонала, описаны правила разграничения доступа, указаны требования к паролям и т.д.

Удалённый доступ

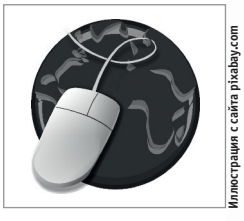
Иллюстрация с сайта pixabay.com

- Не используйте удалённый доступ, если таковой не предусмотрен в целях реализации рабочего процесса. Помните, чтобы удалённым доступом не смог воспользоваться злоумышленник, требуются настройки специализированных средств защиты информации и сетевой инфраструктуры.
- Для удалённого доступа (если таковой разрешён сотруднику официально) используйте сложные пароли и дополни-

тельные процедуры для аутентификации (многофакторную аутентификацию, например).
- Используйте защищённые протоколы передачи данных для удалённого доступа (например, SSL, TLS).
- Отключайте неиспользуемые и ненужные сервисы и службы, чтобы они не стали уязвимым звеном, через которое возможна атака.
- Используйте только персональные средства аутентификации для удалённого доступа.

Мобильные устройства


Иллюстрация с сайта pixabay.com

- Не подключайте мобильные устройства, если это запрещено регламентом.
- Не устанавливайте приложения для мобильных устройств из недоверенных источников.
- Не осуществляйте манипуляции, которые запрещены или влияют на безопасность мобильного устройства (jailbreaking, rooting).

Пароли

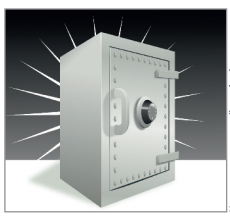
Иллюстрация с сайта pixabay.com

- Проверьте наличие паролей на всех устройствах, интерфейсах контроллеров, схемах SCADA, административных и пользовательских учётных записях средств вычислительной техники.
- Никогда не оставляйте пароли по умолчанию, применяйте сложные и надёжные пароли с наличием специальных символов и разных регистров (если позволяет техническая возможность). Меняйте регулярно пароли.
- Если записали пароль на бумажку, уберите её в надёжное место.

Программное обеспечение, подключения

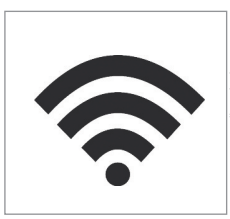
Иллюстрация с сайта pixabay.com

- Используйте на рабочих станциях только ПО, необходимое для выполнения ваших функциональных обязанностей.
- Не открывайте вложения в письмах с незнакомыми расширениями, от незнакомых адресатов. Не игнорируйте предупредительные сообщения от программ.
- Не подключайте непредусмотренные беспроводные устройства в сеть, даже если это очень удобно для вас. Поделитесь с начальством вашими светлыми идеями по оптимизации рабочего процесса. Помните, что беспроводные соединения должны быть соответствующим образом защищены.

Мониторинг событий и оповещение об инцидентах


Иллюстрация с сайта pixabay.com

- Просматривайте журналы событий ОС, прикладных программ и оборудования. Обратите внимание на события, связанные с попытками получения доступа к управлению компонентами АСУ ТП и средствами защиты, с изменениями конфигураций компонентов АСУ ТП, с изменениями прав доступа, с попытками несанкционированного подключения к сетевой инфраструктуре.
- Собирайте и анализируйте статистику работы узлов АСУ ТП на предмет сбоев. Цель – исключить недобросовестных вендоров, которые могут подзарабатывать на «поддержке и восстановлении».
- Сообщайте о подозрительных изменениях в работе ПО и рабочей станции в целом ответственному за защиту информации в АСУ ТП и/или начальству.

Обновление и резервное копирование

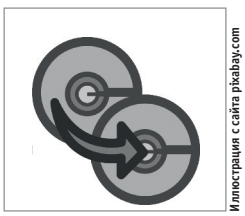
Иллюстрация с сайта pixabay.com

- Регулярно и своевременно обновляйте системное и прикладное ПО, помните, что многие эксплуатируемые уязвимости можно закрыть.
- Помните, что перед установкой обновлений необходимо протестировать их на совместимость с уже установленным программным обеспечением.
- Проводите регулярное периодическое резервное копирование информации, конфигураций программного обеспечения.

Вы должны признать, что ваше предприятие может стать мишенью киберпреступников и обязаны обеспечить выполнение основных мер кибербезопасности, чтобы, как минимум, сделать себя целью посложнее. Это похоже на то, как антилопы сражаются за свою безопасность: вам не нужно обогнать льва, который охотится на вас, чтобы выжить, вам нужно обогнать других антилоп... ●

Литература

1. ICS-CERT MONITOR: May/June 2016 [Электронный ресурс] // ICS-CERT MONITOR. – Режим доступа : https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2016_S508C.pdf.
2. Безопасность АСУ ТП в цифрах [Электронный ресурс] // Positive Technologies. – Режим доступа : https://www.ptsecurity.com/upload/ptru/analytics/ICS-Vulnerability-2016-rus.pdf.
3. Добывающая промышленность становится одной из ключевых целей хакеров [Электронный ресурс] // Anti-Malware. – Режим доступа : https://www.anti-malware.ru/news/2016-08-11/20679.
4. Кибербезопасность промышленных систем: ландшафт угроз [Электронный ресурс] // SecureList. – Режим доступа : https://securelist.ru/analysis/obzor/28866/industrial-cybersecurity-threat-landscape/.
5. Industrial Control System Security. Top 10 Threats and Countermeasures 2016 [Электронный ресурс] // Federal Office for Information Security. – Режим доступа : https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005E.pdf%3bjsessionid=56E8678A780B64F228E0E4989DA3FB35.2_cid369?__blob=publicationFile&v=3
6. Злоумышленники используют бэкдор Gcat для кибератак на энергетические компании Украины [Электронный ресурс] // Хабрахабр. – Режим доступа : https://habrahabr.ru/company/eset/blog/276325/.
7. В компьютерах блока «В» немецкой АЭС было найдено вредоносное ПО [Электронный ресурс] // 3Dnews. – Режим доступа : http://www.3dnews.ru/932167.
8. ICS-CERT MONITOR: January/February 2016 [Электронный ресурс] // ICS-CERT MONITOR. – Режим доступа : https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-Feb2016_S508C.pdf.
9. Wi-Fi, модемы, TeamViewer и прочие ужасы ИБ АСУ ТП [Электронный ресурс] // Zlonov.ru. – Режим доступа : http://zlonov.ru/2016/04/ics-security-horrors/.

E-mail: chernushchenko@gmail.com