Process Safety Beacon
Messages for Manufacturing Personnel
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

This issue sponsored by
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Кибербезопасность и химическое производство

Июль, 2021 г.

Рис.1. Водоочистная станция Олдсмар, Флорида.

5 февраля 2021 г. сотрудник водоочистной станции в Олдсмаре, штат Флорида, заметил, что курсор странно перемещается по экрану управляющего компьютера. Поначалу это его не смутило, поскольку на предприятии использовалось программное обеспечение удаленного доступа для устранения неполадок. Руководитель также часто подключался к компьютеру для мониторинга систем объекта. Позже оператор заметил, что курсор перемещается и щелкает по элементам управления водоочистной установки. В течение секунд злоумышленник пытался изменить заданную подачу гидроксида натрия со 100 частей на миллион (ppm) до 11100 ppm. Оператор быстро обнаружил вторжение и вернул подачу химиката к нормальному уровню. К счастью, на качество воды это не повлияло.

Недавняя атака программ-вымогателей на Colonial Pipeline на несколько дней перекрыла подачу топлива на восточное побережье США.

Системы вашей компании, вероятно, подключены к Интернету и нуждаются в защите от киберугроз. Компании используют множество стратегий для обеспечения кибербезопасности, таких как межсетевые экраны, антивирусное программное обеспечение и политики для защиты от вредоносных программ и компьютерных вирусов.

Все больше людей работают удаленно; это увеличило возможности для кибератак.

Знали ли Вы?

- Киберпреступники используют сложное вредоносное программное обеспечение для достижения своих целей.
- Количество атак с использованием программ-вымогателей увеличивается, поскольку организованные преступники получают от них нелегальный доход.
- Согласно недавнему исследованию, хакерские атаки происходят каждые 39 секунд. (См. Https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Фишинг - это рассылка электронных писем якобы от популярных брендов с целью получение доступа к конфиденциальным данным.
- Киберугрозы могут проникнуть в системы компании через электронную почту, вложения и с портативных запоминающих устройств, таких как USB флеш-накопители.
- 95% нарушений кибербезопасности вызваны человеческим фактором. (См. Https://www.cybintsolutions.com/employee-education-reduces-risk/)

Что Вы можете сделать?

- Прежде чем выполнять обновление программного обеспечения проверяйте запросы с ИТ-отделом, и также своевременно устанавливайте утвержденные обновления.
- Убедитесь, что Ваши брандмауэры и другое сетевое программное обеспечение обновлены и включены.
- Регулярно делайте резервные копии Ваших данных.
- Используйте надежные пароли для любого доступа. Не расскрывайте пароли и регулярно меняйте их.
- Не сохраняйте пароли в браузере.
- Не нажимайте на ссылки или вложения в электронных письмах, отправленных кем-то, кого Вы не знаете.
- Никогда не устанавливайте неутвержденное программное обеспечение на компьютер компании. Убедитесь в защищенности ключей доступа и других физических устройств безопасности.
- Если Вы используете удаленный доступ, следуйте требованиям компании. Будьте особенно бдительны при использовании общедоступных интернет-сайтов.
- Если что-то на Вашем компьютере кажется странным или необычным, обратитесь за помощью! Это может быть хакер, пытающийся получить доступ.

Кибератаки весьма реальны. Вы - жизненно важная часть защиты.