РЕЗУЛЬТАТЫ НАШЕГО ИССЛЕДОВАНИЯ
О СОСТОЯНИИ БЕЗОПАСНОСТИ И
ДОСТИЖЕНИЯ ZENON В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

ПИЩЕВАЯ ПРОМЫШЛЕННОСТЬ БЕРЕТ ИГРУ НА СЕБЯ

Когда дело доходит до новых технологий, пищевая промышленность часто является первопроходцем. Конкурентоспособные предприятия ориентированы на высокую производительность и гибкость процессов. Сегодня заводы все больше и больше автоматизируют свои информационные потоки с целью полной интеграции в них производственного оборудования. Растущие объемы данных фиксируются, передаются и обрабатываются. Отрадно видеть те возможности, которые эта тенденция приносит в отрасль, при этом важно не упустить из вида и новые проблемы в области безопасности, которые приходят вместе с ней.

ДИГИТАЛИЗАЦИЯ ДОЛЖНА БЫТЬ БЕЗОПАСНОЙ

В эпоху цифровой трансформации, автоматизация и IT-платформы играют важную роль в пищевой промышленности, обеспечивая надежность и безопасность при производстве. Наряду с механической и электрическими частями оборудования, программное обеспечение контролирует каждый этап технологического процесса. Правильность вводимых параметров рецепта для достижения ожидаемого качества обеспечивается программным обеспечением, являющимся интерфейсом между оператором и машиной, позволяющим следить за производством в режиме реального времени, анализировать архивные данные и интегрироваться в другие IT-системы. Поскольку программное обеспечение играет такую важную роль, мы должны учитывать, что может произойти без надежных политик в области кибербезопасности.

Представьте себе простую ситуацию, когда неавторизованный человек слегка изменяет некоторые уставки в процессе пивоварения. Результат может оказаться более драматичным, чем просто изменившийся вкус пива. Большое количество дорогих ингредиентов могло быть потрачено впустую, поскольку вся партия могла оказаться испорченной. И что еще хуже, безопасность работы варочного цеха могла оказаться под угрозой.

ОПРОС: КИБЕРБЕЗОПАСНОСТЬ В ПРОИЗВОДСТВЕ НАПИТКОВ

COPA-DATA осознает, какую важную роль играет zenon в многочисленных промышленных приложениях по всему миру. Принятая на себя ответственность в полной мере проявляется в концепции zenon "security by design" и подкрепляется непрерывными инвестициями в безопасность, дающими возможность конечным пользователям, OEM-производителям и системным интеграторам пользоваться высоким уровнем кибербезопасности для своих приложений.

В рамках исследований мы провели опрос представителей почти 230 компаний, которые любезно согласились изложить свою точку зрения на кибербезопасность. Вот что они нам рассказали.

КИБЕРБЕЗОПАСНОСТЬ

в производстве напитков

Среди трендов и инициатив, таких как Индустрия 4.0, Умные Предприятия, Индустрия Вещей и пр., бесспорно выделяется одна тема: **Взаимодействие**

В связи с **ростом потребности** в коммуникациях между машинами, важно сосредоточиться на теме Кибербезопасности. Помимо всего прочего, Кибербезопасность предполагает актуальность систем и установку всех **обновлений безопасности** для защиты их от атак.

ОПРОС

Мы хотели выяснить, представляет ли Кибербезопасность интерес в производстве напитков

приняли участие **228** компаний
(Производство и розлив напитков, пивоварение)

Участвовали предприятия из Германии, Австрии и Швейцарии

Опрашивались компании всех размеров

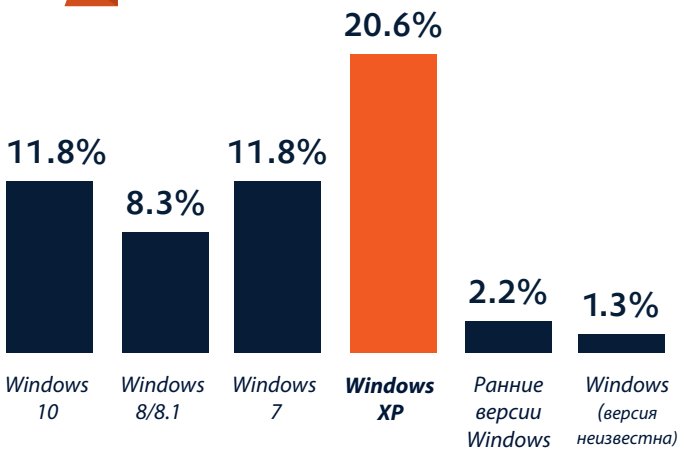
ПРИОРИТЕТ

Значение Кибербезопасности в производстве

Для 55.7% опрошенных, тема Кибербезопасности в производстве имеет низкий приоритет.

Чем больше компания (по объемам производства), тем выше приоритет темы Кибербезопасности в производстве.

ОПЕРАЦИОННАЯ СИСТЕМА WINDOWS



Согласно нашему опросу,

Windows XP

наиболее широко используемая ОС в производстве напитков

Каждая 5ая компания

все еще использует Windows XP. Устаревшие системы представляют существенную угрозу безопасности из-за отсутствия соответствующих обновлений.

ОБЯЗАННОСТЬ

Кто отвечает за Кибербезопасность на производстве?

Отдел производства	**43.0%**
Отдел IT	**19.7%**
Отделы Производства и IT в сотрудничестве	**7.5%**
Отдел производства в сотрудничестве с другим отделом	**3.1%**
Отдел IT в сотрудничестве с другим отделом	**1.8%**
Внешние консалтинговые компании	**8.3%**
CEO или собственники	**5.3%**
Обслуживающий персонал и/или электрики	**1.8%**
Менеджер по качеству или инженер по безопасности данных	**1.3%**
Прочие	**1.3%**
Нет ответа	**7.0%**

Существуют ли в компании стратегии или рабочие процессы по обновлениям систем?

Стратегии и рабочие процессы обновления программного обеспечения достаточно разнообразны. Они зависят от внутренних корпоративных структур, поставщиков, контрактов и возраста оборудования.

СОВРЕМЕННЫЙ УРОВЕНЬ?

Как опрошенные оценивали свое производственное оборудование по сравнению с аналогичными компаниями

Без ответа	**7.5%**
Крайне устаревшее	**2.6%**
Устаревшее	**11.4%**
Среднее	**38.6%**
Современное	**32.0%**
Суперсовременное	**7.9%**

ОБЗОР: КИБЕРБЕЗОПАСНОСТЬ В ПРОИЗВОДСТВЕ НАПИТКОВ – НАШИ РЕЗУЛЬТАТЫ

Как поставщик программного обеспечения, всерьез заботящийся о безопасности своих решений, мы выделили несколько интересных аспектов из результатов опроса.

ПРИОРИТЕТ: ТРЕБУЕТ ПОВЫШЕНИЯ

Когда дело доходит до кибербезопасности, бизнес-риски становятся важными независимо от размеров вашего бизнеса. zenon может помочь всем компаниям, вне зависимости от того, есть ли у вас четкая стратегия кибербезопасности, продвигая тему кибербезопасности прагматично и прямолинейно. Например, zenon позвоялет IT-специалистам внедрять свои политики безопасности и архитектуры - от шлюзов до соответствующих коммуникационных портов. zenon обеспечивает шифрование связи по всем направлениям: по умолчанию для сетевых возможностей zenon и посредством параметров для различных протоколов передачи данных. zenon предлагает надежное управление пользователями с дифференцированной авторизацией, как локально, так и в рамках всего предприятия с развернутым Active Directory. Кроме того, приложения zenon защищены от вредоносных манипуляций посредством цифровой подписи.

Это лишь часть из многочисленных функций безопасности, которые могут помочь предприятиям пищевой отрасли при использовании zenon.

ОТВЕТСТВЕННОСТЬ: ПРОФЕССИОНАЛЬНЫЙ ПОДХОД

Преобладающее мнение опрошенных заключается в том, что производственный отдел должен взять на себя основную ответственность за кибербезопасность. Эти люди уже несут ответственность за производительность, потребление, качество, гибкость и т.д. Действительно, производственный отдел должен определять свои требования к кибербезопсности в той мере, в какой они влияют на защиту конфиденциальных производственных данных, интеллектуальной собственности (например, рецептура продуктов), прав и обязанностей сотрудников, доступности информации и эффективности коммуникации. Однако, кибербезопасность не может быть обеспечена без автоматизации и IT-специалистов. Кроме того, она требует внимания специалистов по техническому обслуживанию, инженеров-электриков и операторов. Эти организационные аспекты должны поддерживаться эффективными программными технологиями, такими как zenon, приносящий безопасность по умолчанию в любое промышленное приложение, будь то управление процессом, контроль производительности, инструмент энергоэффективности или архивирование данных по предприятию и создание отчетности.

ОБНОВЛЕНИЯ: БАЛАНС МЕЖДУ ЗАТРАТАМИ И ПОСЛЕДСТВИЯМИ ДЛЯ БЕЗОПАСНОСТИ

Обновление программного обеспечения часто воспринимается с точки зрения стоимости лицензий, обслуживания и даже интеграционных работ и, собственно, как часть общей стоимости владения (TCO). Чем zenon может помочь здесь? Важно отметить, что

философия COPA-DATA в плане совместимости между версиями значительно упрощает обновление. Во-первых, пользователь сам может решить, когда обновлять версию Среды Исполнения (где запускаются приложения zenon), потому что даже более старые версии остаются с совместимыми с новейшей средой разработки и другими приложениями zenon, которые могут использоваться где-либо в сети. Во-вторых, все нативные компоненты приложения zenon легко конвертировать в новейшую версию - без необходимости модификации. Таким образом, пользователи zenon смогут воспользоваться новейшими функциями безопасности с минимальными усилиями.

ОПЕРАЦИОННЫЕ СИСТЕМЫ WINDOWS: ПРОДЛЕНИЕ ЖИЗНЕННОГО ЦИКЛА МАШИН

Один поразительный вывод из нашего опроса, заключается в том, что каждая пятая компания по-прежнему использует Windows XP - операционную систему, поддержка которой была прекращена много лет назад, что увеличивает вероятность наличия уязвимостей в системе безопасности. Производственные предприятия, продолжающие использовать ее, подвержены высокому риску из-за всех машин и систем, работающих под Windows XP, а также подключенных к ним для сбора данных или с целью удаленного технического обслуживания.

Высокая степень коммуникации, присущая оцифрованному производству, говорит о необходимости иметь четкий план обновления установленных операционных систем. zenon всегда отвечает современным требованиям и совместим с новейшими операционными системами семейства Windows. Это помогает производственным отделам продлить жизненный цикл их машин, обеспечивая таким образом готовность к решению задач по дигитализации.

СОВРЕМЕННЫЙ УРОВЕНЬ: ПИЩЕВАЯ ПРОМЫШЛЕННОСТЬ ИГРАЕТ ВЕДУЩУЮ РОЛЬ

Наше исследование в области кибербезопасности заканчивается на позитивной ноте - по оценке большинства участников они используют современное оборудование. Это согласуется с идеей о том, что динамическая Пищевая Промышленность является лидирующей и, как правило, внедряет новые технологии на ранней стадии. В настоящее время перед отраслью стоит задача продемонстрировать свое лидерство в важном вопросе кибербезопасности путем внедрения современных технологий безопасности.

Тема кибербезопасности приносит не только проблемы, но и перспективы. Важное значение имеют повышение компетентности и постоянное совершенствование стратегий безопасности. Мы видели, как zenon может помочь, но тем не менее, здесь, в COPA-DATA, наше путешествие продолжается. Мы будем продолжать развивать тему киберезопасности с помощью новых исследований, усовершенствования продукта, специальных тренингов и многих других инициатив. В августе 2018 года, COPA-DATA была сертифицирована в соответствии со стандартом безопасности IEC 62443.

Будьте в курсе наших новостей о кибербезопасности и подпишитесь на нашу рассылку, посвященную Пищевой Промышленности.

ЭМИЛИАН АКСИНИЯ,
руководитель направления
пищевой промышленности