Проблемы информационной безопасности и их решение при использовании офисных печатающих устройств

Москва, 18 ноября 2021 г. — Информационное Агентство «Бизнес-Информ» и Ассоциация Производителей и Поставщиков Качественных Расходных Материалов представили результаты исследований уязвимостей офисных печатающих устройств и рекомендации по их устранению.

Информационное Агентство «**Бизнес-Информ**» и Ассоциация Производителей и Поставщиков Качественных Расходных Материалов (**АППКРМ**) 18 ноября текущего года провели конференцию **«Проблемы информационной безопасности и их решение при использовании офисных печатающих устройств в корпоративных сетях».** На конференции были продемонстрированы результаты исследований уязвимостей офисных печатающих устройств, обнаруженные в российских и зарубежных организациях в 2018-2021 годах, а также рекомендации по их устранению. Особое внимание на конференции было уделено современным политикам информационной защиты корпоративных сетей предприятий, а также вопросам, связанным с практикой эксплуатации систем документооборота (ИТ-аутсорсинг, MPS, использование восстановленных картриджей и картриджей-новоделов). В конференции приняли участие представители 144 российских предприятий и организаций, а также ведущие российские и зарубежные эксперты в области информационной безопасности.

На конференции были заслушаны 4 доклада:

- **«Пандемия COVID-19 меняет и повышает требования к информационной безопасности»** (докладчик — Малинский С.В., Российский Университет Транспорта)

Тезисы доклада: Рост киберпреступности в период пандемии COVID-19 – общемировая проблема. Рост заболеваемости, переход на работу из дома, появление новых уязвимостей, рост числа и интенсивности кибератак. Статистика киберпреступности в 2020-2021 годах. Под ударом – все отрасли экономики, но особенно – здравоохранение и финансы. В период с марта по май 2020 года посещаемость хакерских сайтов и форумов выросла на 66%. Удаленная работа порождает новые уязвимости, в том числе и через домашние принтеры. Тренд последних лет – переход преступников на аутсорсинг, появилась схема «преступление как услуга» (crime as a service)». Трансформация политики информационной безопасности необходима. Перспективы новой политики ИБ на основе принципа «нулевого доверия» (Zero Trust). Печатающие устройства и их уязвимости. Новые требования к контролю за печатающими устройствами. Картриджи тоже несут уязвимости..

- **«Преступники объединяются, а киберугрозы нарастают»** (докладчик — Малинский С.В., Российский Университет Транспорта)

Тезисы доклада: Рост преступности в период пандемии COVID-19 – общемировая проблема. Гибридные формы организации труда, внедрение облачных технологий, развитие ИТ-аутсорсинга, увольнения сотрудников служб ИБ, обиженные в ходе обязательной вакцинации сотрудники - вот лишь небольшая часть "мелочей", на которых стремительно развивается современная киберпреступность. Тренд последних лет – переход преступников на аутсорсинг. Широкое распространение в Интернете предложений к продаже программ-вымогателей-в-качестве-услуги (RaaS, ransomware-as-a-service). Многоуровневый список предлагаемых вредоносных пакетов ПО, от «пробного» пакета на месяц за 90 долларов до «элитного» подписного пакета на 12 месяцев со за 1400 долларов. Криминальные группы, создающие подобные сайты, работают по принципу продаж лицензионных моделей. Киберпреступность создает новые рабочие места. Появление тематических сайтов с продукцией для кибермошенничества стало драйвером для роста числа низкоквалифицированных участников хакерского сообщества. Новые киберугрозы с использованием программ-вымогателей (ransomware). Печатающие устройства создают новые уязвимости.

- **«Принципы, компоненты и проблемы нулевого доверия»** (докладчик – Малинский С.В., Российский Университет Транспорта)

Тезисы доклада: Рост преступности в период пандемии. Zero Trust («нулевое доверие») – это модель безопасности, предполагающая полное отсутствие доверия к какому-либо пользователю, устройству, приложению. Основные компоненты архитектуры нулевого доверия согласно «NIST Special Publication 800-207: ZeroTrust Architecture». Требования нулевого доверия к операционным системам и устройствам ввода/вывода и их функционалу. Обновление ПО как новый источник уязвимостей. Оригинальные и неоригинальные картриджи несут новые угрозы. Превентивные меры защиты. Необходимость непрерывного мониторинга сети. Если кража информации неизбежна, на помощь приходит стеганография. Уточнения существующих политик информационной безопасности неизбежны. Тенденции развития российского рынка офисной печати в новых условиях.

- **«Принтеры, МФУ и картриджи – источники уязвимостей. Рекомендации по приобретению, эксплуатации и утилизации. Ответственность поставщиков и пользователей в соответствии с законодательством РФ»** (докладчики — Семенов А.И., Юридическое Агентство «Бизнес-Информ», Савинова А.А., Информационное Агентство «Бизнес-Информ»)

Тезисы доклада: Офисная печать и ее организация: программно-технические аспекты. Дыры в системном и прикладном программном обеспечении. Патчи и их роль для хакеров и специалистов по ИБ. Принтеры и МФУ как источники уязвимостей. Решения производителей печатающих устройств и можно ли им доверять? Сертификаты по ИБ печатающих устройств и какое отношение они имеют к российскому рынку. Встроенное ПО и его обновление. Какие цели преследуют производители? Удаленные рабочие места приносят новые проблемы. Картриджи (оригинальные, восстановленные и новоделы) и чипы – еще одни группа вопросов по ИБ. Что делает чип: заявления изготовителей и мнение исследователей по ИБ. Шпионская техника и что о ней написано в УК РФ и КоАП РФ. Обзор судебной практики, начиная с 13 августа 2019 года. Ответственность поставщиков и ответственность пользователей. Проблемы утилизации печатающих устройств и расходных материалов для специалистов по ИБ: обзор ошибочных решений и рекомендации по практической деятельности в 2022 году.

Участники конференции обсудили с докладчиками представленную информацию, результаты исследований уязвимостей офисных печатающих устройств, обнаруженные в российских и зарубежных организациях в 2018-2021 годах, а также рекомендации по их устранению. Особое внимание участники конференции уделили современным политикам информационной защиты корпоративных сетей предприятий, а также вопросам, связанным с практикой эксплуатации систем документооборота (ИТ-аутсорсинг, MPS, использование восстановленных картриджей и картриджей-новоделов). Приятным подарком для всех участников конференции стали новые выпуски журнала BUSINESS-INFORM Review (выпуск №32, 2021) и его приложения «Экспертиза и Качество» (октябрь, 2021).

АППКРМ: info@aqcmsrus.ru, https://aqcmsrus.ru/

БИЗНЕС-ИНФОРМ: bizinform@list.ru, http://sforp.ru/