КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КОД ИБ | СПБ

27.04.2023

Йоханн Воронин

- Бизнес-Информатика, университет Дортмунд
- PMP®, Project Management Institute
- Scrum Master® & Product Owner®
- Специалист по информационной безопасности и политики конфиденциальности персональных данных

Cybercrime-Trends 2023

Top 5 Cybercrime-Trends 2023

01 artificial intelligence

Технологии дипфейков и клонирование голоса и создания правдоподобных видео

Автоматический подбор пароля и взлом CAPTCHA

Генеративное ИИ пишет фишинговые письма лучше чем человек* и генерирует вредоносный код

*Singapore, Government Technology Agency, 2021

02 Social Engineering

Фишинг (**Phishing**) и социальная инженерия (**Social Engineering**) остаются излюбленными методами атак и получают дальнейшее развитие.

Манипулирование эмоциями своей жертвы, чтобы украсть конфиденциальную информацию.

Создание чувства доверия, авторитета, дефицита или срочности

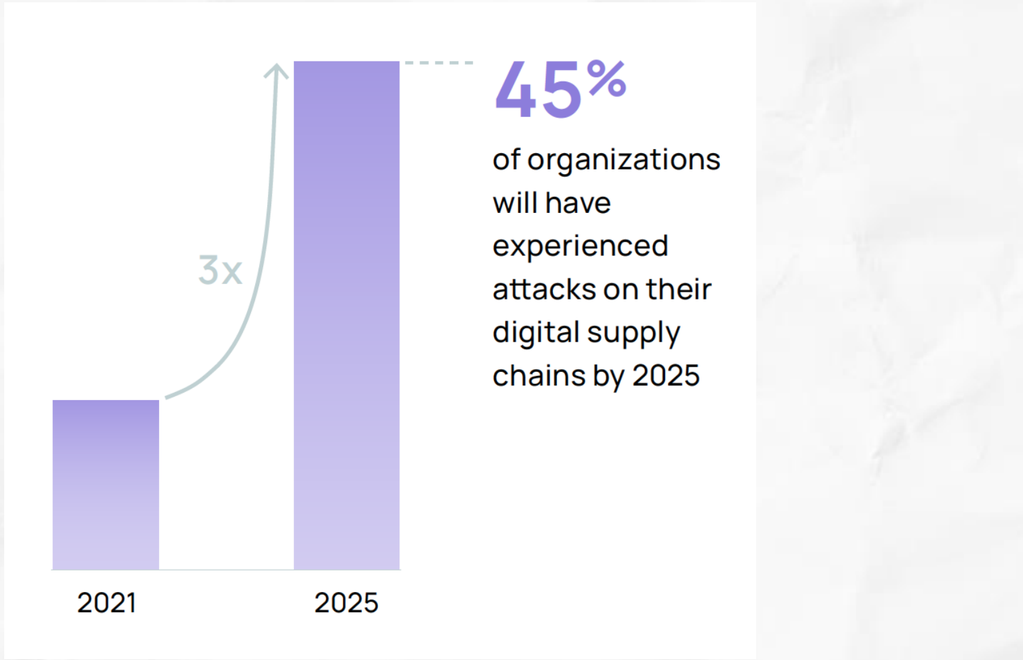
03 Ransomware-asa-Service

ENISA (European Union Agency for Cybersecurity) говорит о «золотой эре программ-вымогателей», т.н. **RANSOMWARE**. **Сложные тактики атак, такие как множественный шантаж**, увеличивают риск неправомерного использования данных почти на 800%.

По данным AV-Test, количество вредоносного ПО также достигло нового максимума в 2021 году — было обнаружено более 150 млн вариантов вредоносных программ, 59% из которых — трояны.

04 Digital Supply Chain Attacks

Крупномасштабные атаки на цепочки поставок (**Supply Chain Attacks**) нацелены на слабые звенья и наносят ущерб всей системе поставок.



05 Multi-factor authentication fails

- MFA push spam (Uber, MS, Cisco)
- Метод атакующего посередине (AiTM)
- Подмена SIM карт
- Вредоносное ПО удерживающее сеанс после выхода пользователя

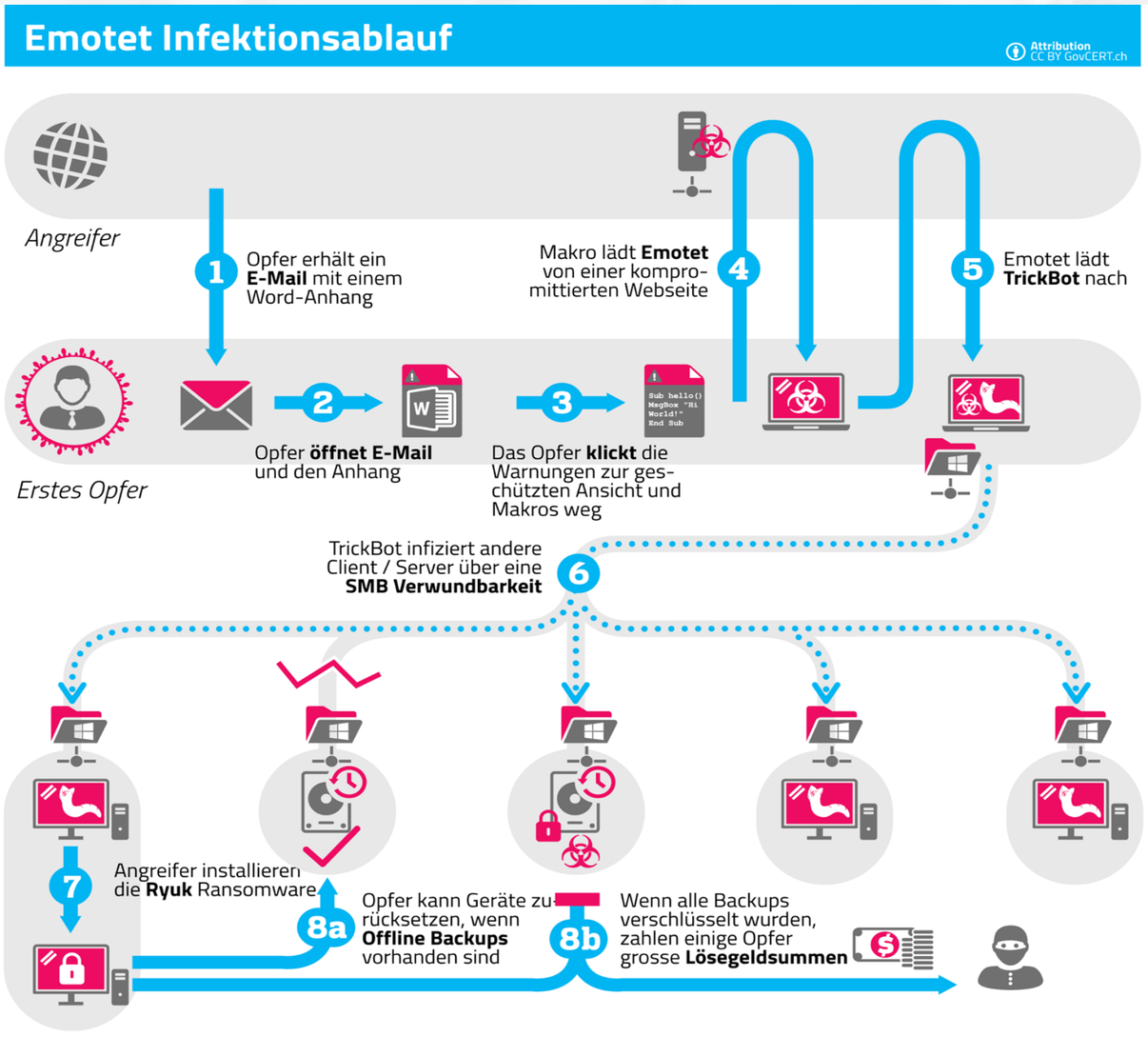
Сектора под прицелом

Ритейл

Срочная цифровизация и глобальные сетевые цепочки поставок

Закрытие магазинов из-за карантина и увеличение количества онлайн-заказов сместили многие процессы в цифровое пространство. Многие местные ритейлеры выходят в онлайн-бизнес впервые и зачастую еще недостаточно подготовлены к связанным с этим рискам.

Ритейл - пример IKEA



Незадолго до Рождества 2021 года шведский производитель мебели IKEA стал мишенью киберпреступников. Они использовали настоящие адреса электронной почты IKEA для рассылки вредоносных программ, таких как **Emotet** или **Qbot**, внутри компании или партнерам по цепочке поставок.

Производство

Индустрия 4.0, дорогостоящие остановки производства и эксклюзивные нематериальные товары

Несколько лет назад компании-производители все еще чувствовали себя в относительной безопасности от кибератак. Но после комплексной оцифровки в контексте Индустрии 4.0 появились новые цели.

Производство - пример Eberspächer

Октябрь 2021. Крупнейший поставщик автомобильной электроники. Атака затронула ИТ-инфраструктуру; веб-сайт был временно недоступен, все ИТ-системы были отключены в целях остановки атаки..

Финансы

Конфиденциальные данные и все более строгое регулирование

Уже на первом этапе блокировки в период с февраля по апрель 2020 года было очевидно, что киберпреступники используют этот поворотный момент: количество кибератак на финансовый сектор выросло на 238 процентов. Конфиденциальные и личные банковские данные клиентов могут быть проданы на черном рынке за огромные суммы.

Финансы - пример CNA Financial

Атака попала в заголовки в основном из-за выкупа. CNA Financial выплатила крупнейший на сегодняшний день выкуп в размере **40 миллионов долларов** после инцидента с программой-вымогателем.

Государственный сектор

Повышенное внимание СМИ как средство давления

ИТ-инфраструктура в государственном секторе зачастую устаревшая, что позволяет профессиональным злоумышленникам легко получить к ней доступ. Интерес СМИ к подобным случаям достаточно велик.

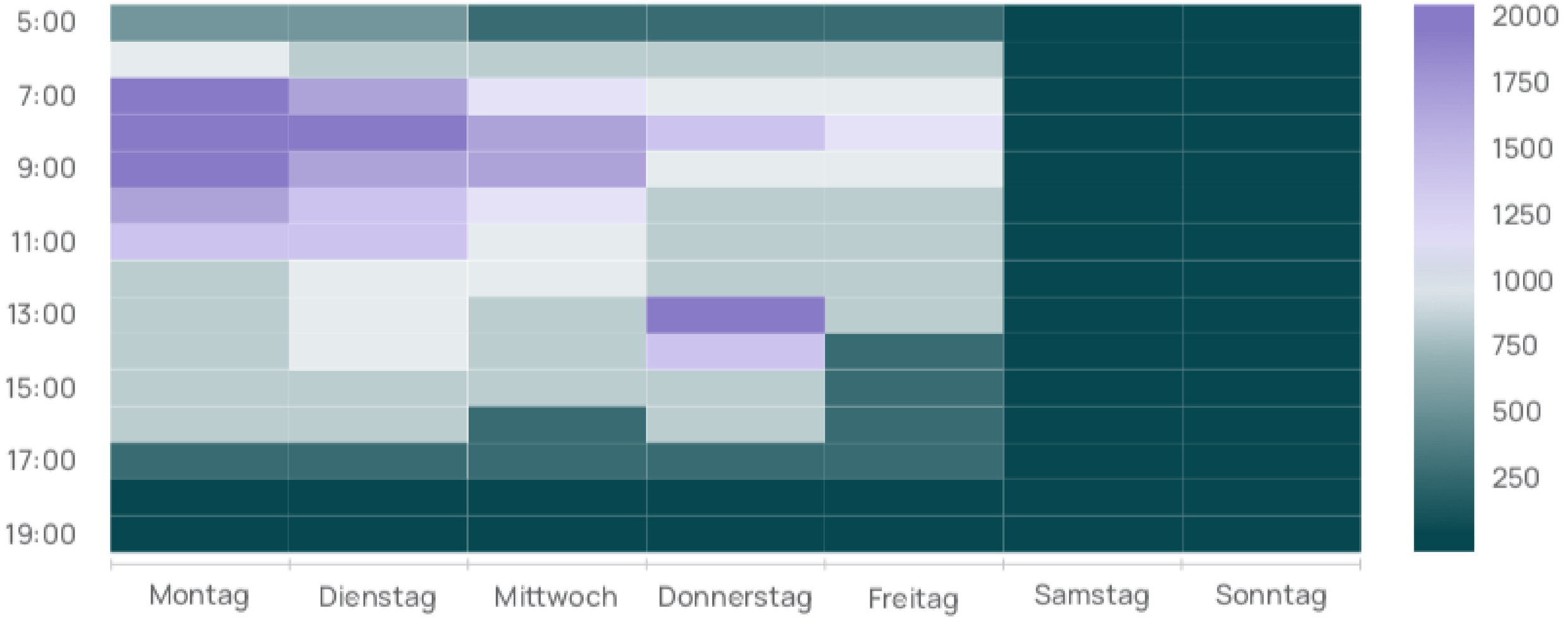
В конце концов, многие граждане зависят от услуг местных органов власти, таких как выплаты пособий или регистрация транспортных средств.

Государственный сектор - пример Bitterfeld

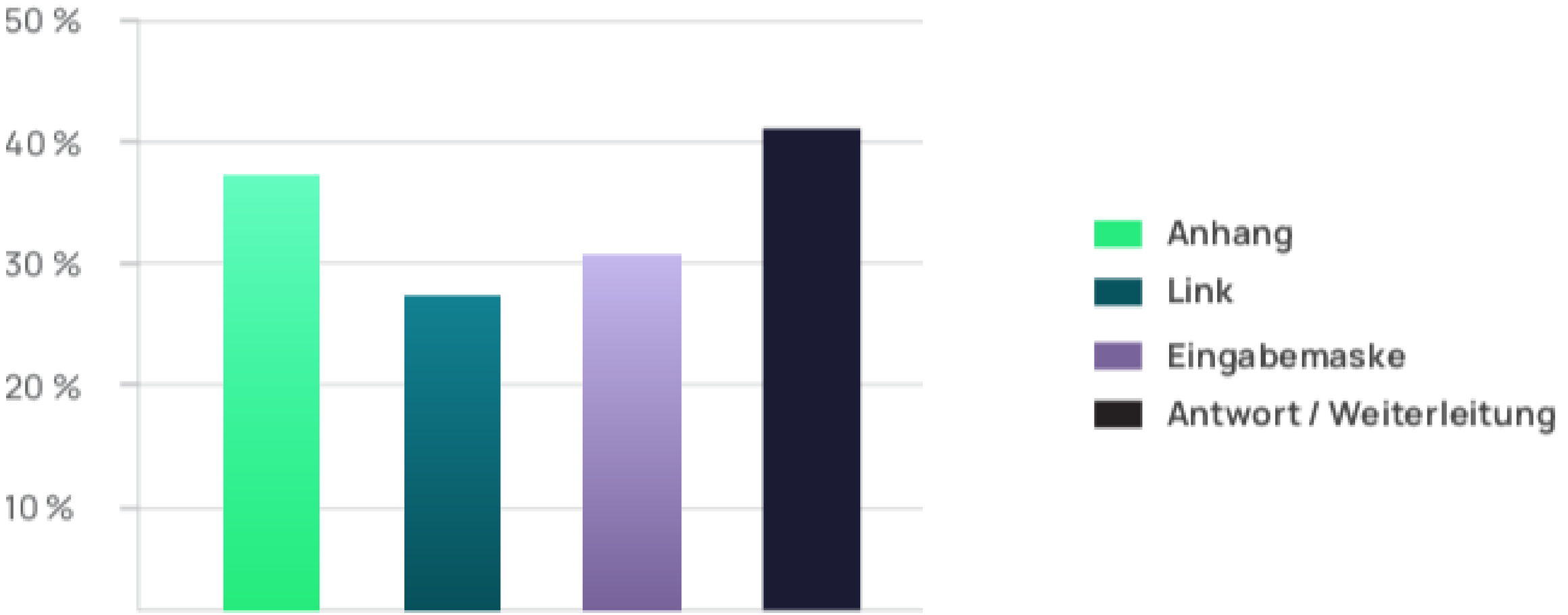
В июле 2021 года несколько серверов Биттерфельда были заражены программой-вымогателем, в результате чего был зашифрован большой объем данных. Регистрация транспортных средств, заявления на родительское пособие и многие другие услуги больше не могли быть обработаны.

Немного статистики

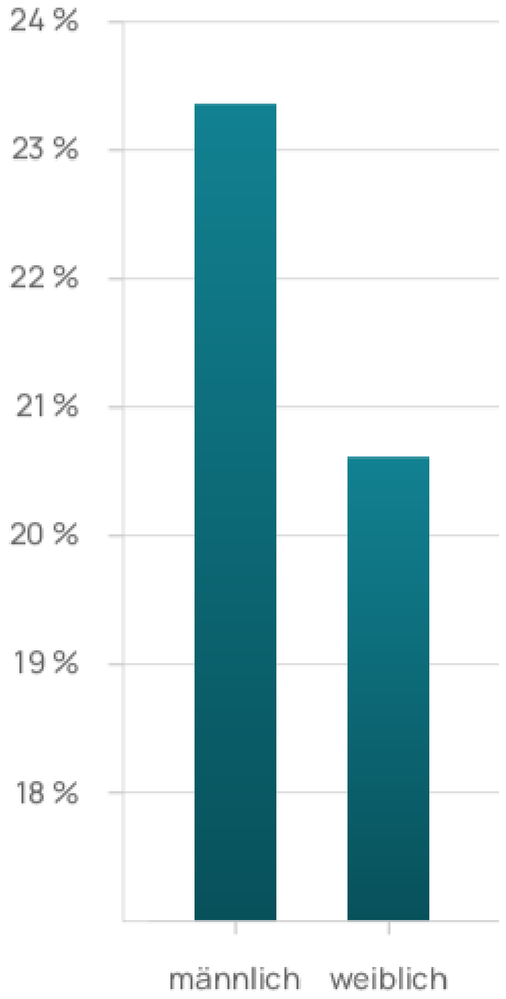
Кто рано встаёт… тот на крючке

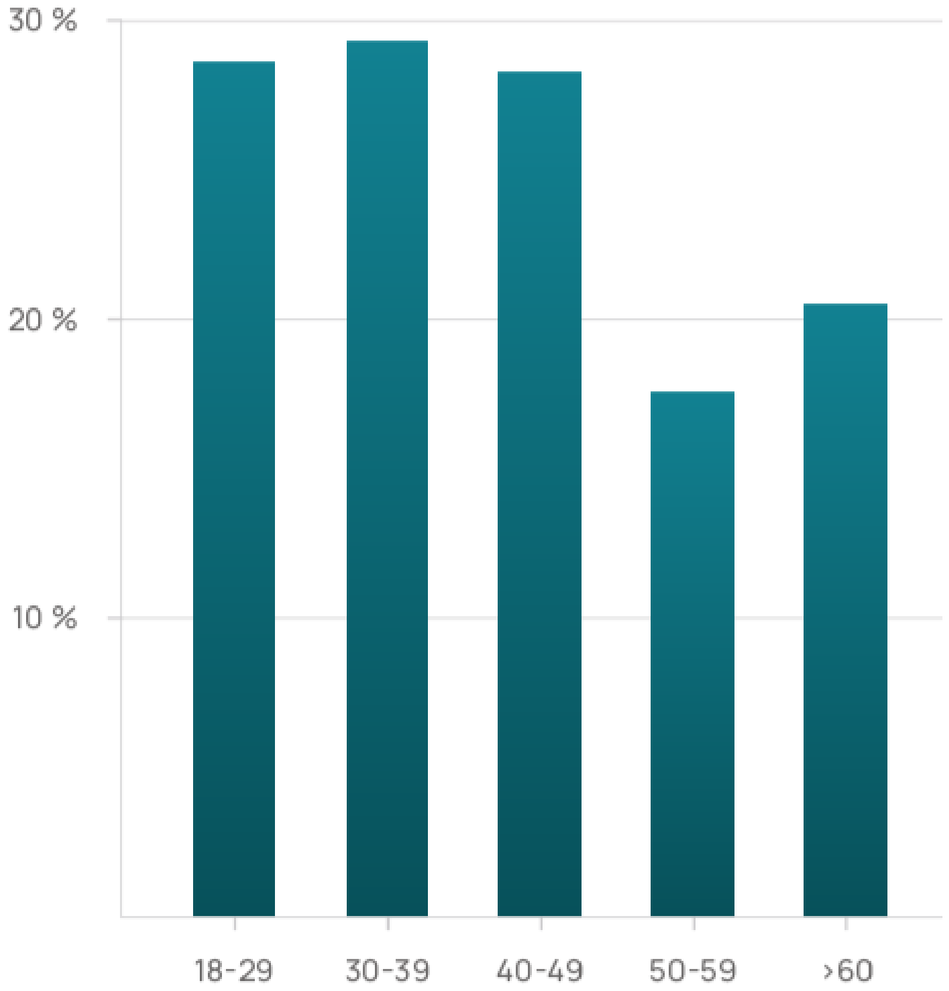


>40% отвечают или пересылают



Пол и возраст





Технические и организационные мероприятия

Представленная «Модель поведенческой безопасности» имеет четыре измерения, все из которых следует рассматривать в равной степени.

Концепция

Знания

Мотивация

Поведение

Готов ответить на ваши вопросы

E-mail: johann.voronin@korbit.ru
Phone: +7 906 219 66 00