



КОД ИБ

ТЮМЕНЬ

ШТАБНЫЕ КИБЕРУЧЕНИЯ

04 апреля 2024

Тюмень



ВЛАДИМИР МАКАРОВ

Руководитель направления ИБ
Кошелёк

Коротко о себе

- 10+ лет практического опыта работы в области ИБ
- 5+ лет опыта руководства подразделениями ИБ
- **ISO/IEC 27001 Lead Auditor**
- **Certified Ethical Hacker (CEH)**
- Аудитор по ГОСТ Р 57580 (АБИСС)
- Руководитель направления ИБ в компании «Кошелёк»



Кошелек — приложение, с которым покупают

12 млн

Человек каждый день
пользуются Кошельком

230

Сотрудников в штате

414+ млн

Карт выпущено и добавлено
в приложение

525 тонн

Оцифрованного пластика



Зачем проводятся киберучения

- Разработка или проверка работоспособности планов реагирования на инциденты ИБ
- Симуляция последствий инцидентов для возможности проведения адекватной оценки рисков ИБ
- Формирование у специалистов понимания серьезности инцидентов ИБ





ИНЦИДЕНТ № 1
ФИШИНГ 80 УРОВНЯ

Наша компания ООО «Инновация сервис»



- Компания оказывает аутсорсинг IT услуг
- Штат 150+ человек
- Внедрена СУИБ
- Имеется отдел ИБ

Инцидент № 1

К вам утром приходит сотрудник и сообщает, что получил вот такое письмо:



Сдача отчетности

1С Support <1c.help2017@gmail.com> 🔍

21 декабря, 4:30



Здравствуйте, Ольга Венедиктовна!

Для использования новых функций сдачи отчетности ООО "Вектор", необходимо установить расширение для Вашей версии 1С.

Для этого перейдите по [ссылке](#) и следуйте указаниям на экране.

Предупреждаем, что в случае использования программы 1С без данного расширения, возможны сбои в сдаче отчетности в ФНС.



С уважением, служба поддержки 1С.

Какие риски несет инцидент?



РИСКИ:

- 1) Утечка информации
- 2) IP адрес
- 3) ПО
- 4) Сбор информации о типовой системе пользователя
- 5) Потеря домена
- 6) Шифрование

Наши действия?



Действия:

- 1) Опросить сотрудников: случилось ли что-то после этого?
- 2) Блокировка по служебным заголовкам
- 3) Предупредить сотрудников об атаке!!!**
- 4) Принять решение об уведомлении НКЦКИ
- 5) Блокировка файла (поиск индикатора)
- 6) Инициировать смену паролей

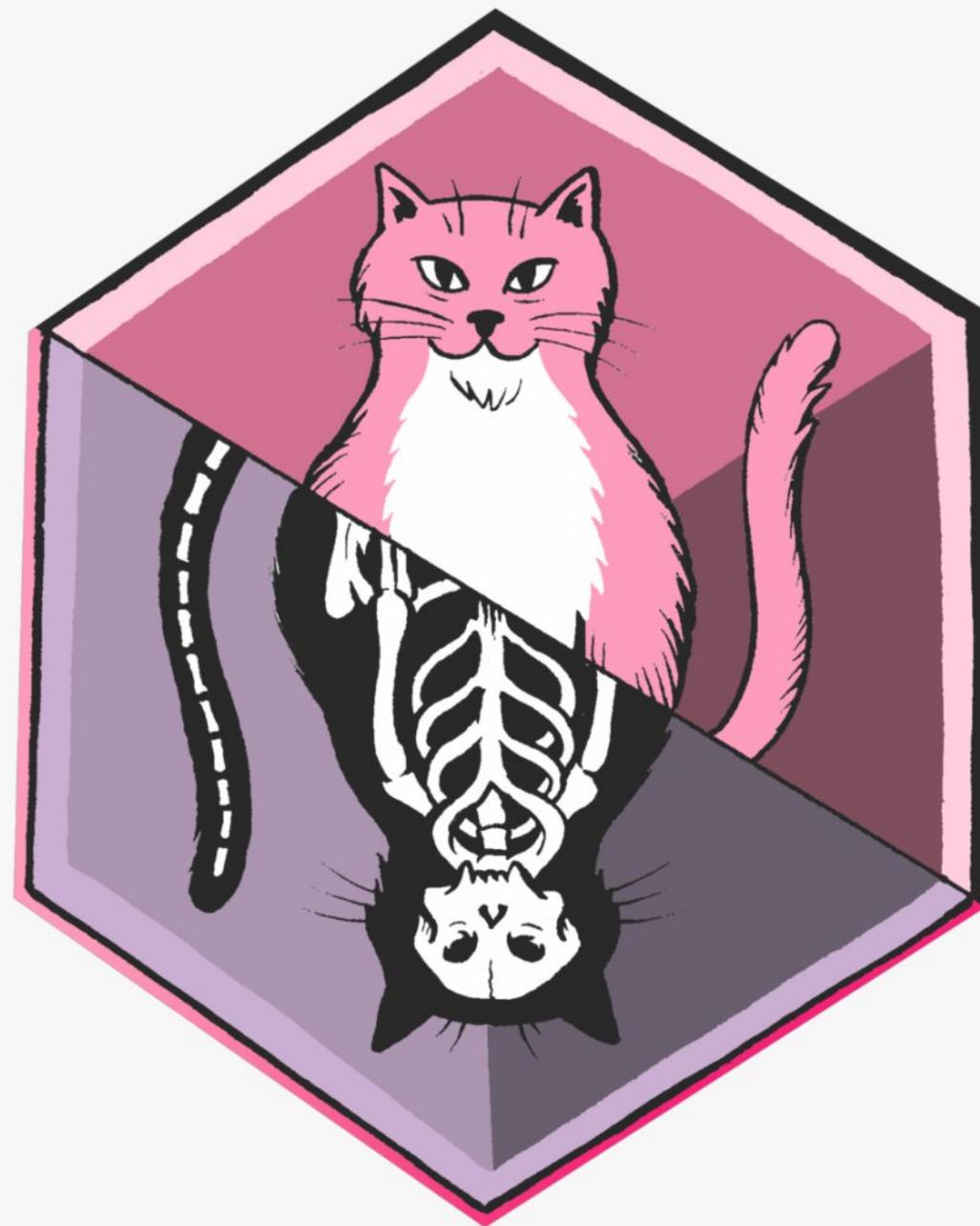
Вы заходите в антиспам систему на почтовом сервере и видите там более 1000 различных детектов за прошедшие сутки

Средний месячный показатель по вредоносным письмам – не более 100 в месяц



ИНЦИДЕНТ № 2

УТЕЧКА ШРЁДИНГЕРА



Наша компания ООО «Интернет трейд»



- Компания e-commerce
- Штат 200+ человек
- Внедрена СУИБ
- Имеется отдел ИБ
- Внедрен процесс AppSec
- Сайт защищен WAF и от DDoS
- Ваш сайт bestshop.ru
- Ваш магазин имеет много маркетинговых акций с другими компаниями

Инцидент № 2

К вам приходит сотрудник и сообщает, что пытался «пробить» знакомую через «Глаз Бога» и там увидел:

ПОЛЬЗОВАТЕЛИ BESTSHOP.RU 2024

ФИО:	Иванов Иван Иванович
День рождения:	08.06.1997
Адрес:	Рязань
Телефон:	79999599329
ID операции:	32161354417
ID клиента:	10142723144
Группа:	Клиенты
Дата создания:	2022-06-08 02:02:00
Возраст:	26 лет

Какие риски несет инцидент?



РИСКИ:

- 1) Репутационные
- 2) Утечка ПДн
- 3) Финансовые
- 4) Судебные
- 5) Внимание регулятора

Наши действия?



Действия:

1) Проверить действительно ли была утечка по актуальным ID (Взломали ли наши системы?)

2) Опросили DATA-инженеров

3) Поднять все средства защиты

4) Сверить данные (названия полей, поля ID операции, код клиента)

5) Инициировать встречу с департаментом ИБ партнёра

6) Внести изменения в договор с партнёрами

ПОЛЬЗОВАТЕЛИ BESTSHOP.RU 2024

ФИО:	Иванов Иван Иванович
День рождения:	08.06.1997
Адрес:	Рязань
Телефон:	79999599329
ID операции:	32161354417
ID клиента:	10142723144
Группа:	Клиенты
Дата создания:	2022-06-08 02:02:00
Возраст:	26 лет

Попросив сотрудника выгрузить полный отчет «Глаза Бога» вы замечаете:

ПОЛЬЗОВАТЕЛИ BESTSHOP.RU 2024

ФИО: Иванов Иван Иванович

День рождения: 08.06.1997

Адрес: Рязань

Телефон: 79999599329

ID операции: 32161354417

ID клиента: 10142723144

Группа: Клиенты

Дата создания: 2022-06-08 02:02:00

Возраст: 26 лет

ПОЛЬЗОВАТЕЛИ LIVESPORT.RU 2024

ФИО: Иванов Иван Иванович

День рождения: 08.06.1997

Адрес: Рязань

Телефон: 79999599329

ID операции: 32161354417

ID клиента: 10142723144

Группа: Клиенты

Дата создания: 2022-06-08 02:02:00

Возраст: 26 лет

Проверив Telegram каналы с утечками вы узнаете что у партнера LiveSport совсем недавно была утечка клиентской базы

Утечки информации

46.0.1	0	登录成功	2023-03-22 19:13:28	6c13824a7cba8289752b245d9617139a	Rus	
185.36	0	登录成功	2023-03-24 00:57:04	b741d7cebf9e697097f2f36609b9a7a4	Rus	
46.72.	0	登录成功	2023-03-22 00:33:44	9746e44aec573100fdded7faf7beb1992	Rus	
185.45	0	登录成功	2023-03-23 23:11:23	a7a15c509b1f892c066f5fa967e051b7	Rus	
176.55	0	登录成功	2023-03-23 21:00:52	e7bee0d54414fc6999e138ca8a3a39d0	Rus	
176.21	0	登录成功	2023-03-20 04:48:50	7173221ebfa8f013f498a70ad801b20e	Rus	
178.34	0	登录成功	2023-03-23 21:00:00	0b5ecc70cf7efc4d5950497fcb8c7f58	Rus	
188.16	0	登录成功	2023-03-20 21:56:23	47eb641c27fa4e1c19c37ab95420e048	Rus	
5.164.	0	登录成功	2023-03-22 17:33:27	47eb641c27fa4e1c19c37ab95420e048	Rus	
l.com	193.16	0	登录成功	2023-03-21 18:20:56	569583FC-E818-4DE8-A786-E3098CF3E360	Rus
94.19.	0	登录成功	2023-03-20 20:43:33	04e7f097febFd40423e2443e8342dd15	Rus	
85.14e	0	登录成功	2023-03-22 20:41:05	c10211111111111111111111111111111	Rus	
213.87	0	登录成功	2023-03-21 16:38:14	F55e10E8011111111111111111111111	Rus	
31.172	0	登录成功	2023-03-21 08:54:49	67640f5d01ec429e9406a5b1ab5cdf72	Rus	
188.0.	0	登录成功	2023-03-23 17:08:22	2c6fcecb34f9058c080a9dcaa8dcfc26b	Rus	
91.193	0	登录成功	2023-03-22 22:11:25	862744fc578377067b7d6178b65a0003	Rus	

NR	Willy	PO242108862556	Order enquiry:PO242108862556	refund pls
	Evan	PO242088809822	Order enquiry:PO242088809822	How can i
	Xylas7	PO24210667086	Order enquiry:PO24210667086	I just wan
	Ondra	PO24206079378	Order enquiry:PO24206079378	change siz
	Mars	PO24205610991	Order enquiry:PO24205610991	Hi i order
XX	Yilia	PO24211734208	Order enquiry:PO24211734208	shipping a
	Jade	PO24214275703	Order enquiry:PO24214275703	HI im just

В открытый доступ был выложен частичный дамп базы данных покупателей маркетплейса livesport.ru

В трех текстовых файлах находятся данные за период с 20.03.2023 по 21.03.2024.

К России относится около 5,2 тыс. записей (из более чем 3 млн):

- имя/фамилия
- адрес эл. почты
- телефон
- адрес
- IP-адрес
- номер заказа
- текст обращения в поддержку

24.6K изменено 11:10

ИНЦИДЕНТ № 3*

**ВСЕ ПРОПАЛО
МИХАЛЫЧ!**



Наша компания ООО «НеИнновация сервис»



- Компания оказывает аутсорсинг IT услуг
- Штат 150+ человек
- СУИБ не внедрена
- Нет отдела ИБ

Инцидент № 3*

Утро понедельника.
Вы приходите на работу и
вдруг видите что вся
Windows инфраструктура -
зашифрована



Какие риски несет инцидент?



РИСКИ:

- 1) Целесообразность существования организации
- 2) Ущерб данных
- 3) Материальный ущерб
- 4) Ущерб инфраструктуры
- 5) Утечка данных
- 6) Репутационные
- 7) Угроза атаки на клиентов
- 8) Невозможность определения доступа к вашей инфраструктуре

Наши действия?



Действия:

- 1) Предупредить клиентов, оборвать сетевые связи
- 2) Проверить бэкапы
- 3) Наличие дешифратора
- 4) Попросить помощи у вендора
- 5) Сообщить в соответствующие органы об инциденте
- 6) Попытаться расшифровать
- 7) Поиск источника
- 8) Проверка бэкапов на то, что они не заражены
- 9) Сканирование на наличие маркеров компрометации
- 10) Восстановление с бэкапов 2,3 уровня (если они есть)

Макаров Владимир

Спасибо за внимание!

