SAVE IT group

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Если не взломаем Мы, то взломают Вас

Директор по развитию бизнеса SaveIT Group
Анна Попенко

Предпосылки

2017 Data Breach Investiatins Repirt

		Accommodation	Education	Finance	Healthcare	Information	Manufacturing	Public	Retail	Accommodation	Education	Finance	Healthcare	Information	Manufacturing	Public	Retail
Pattern	Denial of Service	4	228	445	3	508	10	617	180				1	2		1	
	Privilege Misuse	5	7	48	125	23	13	7,417	9	5	5	26	104	13	8	58	6
	Lost and Stolen Assets	5	13	10	92	4	2	5,519	4	4	3	2	42	2	1	7	
	Everything Else	8	106	20	40	32	213	88	8	8	14	16	28	24	4	19	3
	Point of Sale	182		3	4	1			9	180		3	3				8
	Miscellaneous Errors	2	24	14	114	13	3	2,246	16	1	16	10	96	9	2	38	12
	Web App Attacks	4	25	376	32	73	4	148	28	3	11	364	15	61		13	24
	Crimeware	5	32	30	54	63	261	5,102	14		5	7	12	1	2	5	1
	Payment Card Skimmers	6		53			1	1	57	5		44				1	39
	Cyber-Espionage		22	5	2	4	115	112	3		19	5	1	4	108	98	1
Action	Hacking	176	394	850	84	616	588	958	220	171	43	387	48	89	111	130	30
	Misuse	5	7	48	125	23	13	7,417	9	5	5	26	104	13	8	58	6
	Physical	12	11	64	73	4	2	18	62	10	2	46	31	2		11	39
	Social	9	131	385	37	47	390	147	24	9	32	372	23	37	109	102	20
	Error	2	28	18	154	16	5	7,763	16	1	19	11	119	10	3	47	12
	Malware	187	58	395	66	111	358	5,219	42	180	26	370	18	42	92	103	24
	Environmental																
Asset	Server	185	367	874	184	634	68	880	234	175	34	399	123	101	10	100	38
	Media	8	12	14	145	6	1	1,440	11	7	5	10	105	5	1	31	8
	User Dev	178	43	393	76	50	302	5,691	36	174	18	367	25	34	63	109	23
	Person	10	132	387	41	48	390	149	24	10	33	372	27	38	109	104	20
	Network		2	6	3	6		3				1		2		1	
	Kiosk/Terminal	4		57			1	2	57	3		45				1	38
	Embedded																

0% 25% 50% 75% 100%

Crimeware

Отрасль: гос. активы и производство/добыча

2017 год: 6925 инцидентов

Источник данных об инцидентах: Computer Emergency Response Teams (CERTs) или Computer Security Incident Response Teams (CSIRTs)

На что нацелен хакер?

Программный модуль

Готовое программное обеспечение

Прикладные и системные сервисы/службы

Протокол взаимодействия (сеть, wif и т.п.)

Информационная система

Персонал

К чему приводит взлом?

Март 2018 г.
Взлом приложения MyFitnessPal
Утечка ПДН 150 млн. пользователей.

Октябрь 2017 г.
Bad Rabbit («Плохой кролик»)
Атаковал сайты ряда российских СМИ («Интерфакс», «Фонтанка»).

Май 2017 г.
WannaCry
Атакам подверглись системы МЧС, МВД, РЖД, Сбербанка, «Мегафон» и «Вымпелком».
Ущерб 7 млн. рублей.

Июнь 2017 г.
Petya (или NotPetya)
В России атака «Роснефти», «Башнефти», «Евраза», российских офисов компаний Mars, Mondeles и Nivea.

Июнь 2017 г.
Хакерская атака
Пенсионный фонд РФ, утечка персональных данных более 17 тыс. человек.

Март 2017 г.
Хакерская атака
Столичных банков – Пострадал «Тексбанк».
Ущерб 27 млн. рублей.

Что диктует жизнь?

- Даже малый бизнес может быть привлекательным для кибермошенников;
- Убытки от утечек несоизмеримо дороже цены анализа защищённости;
- Утечка коммерческой тайны может остановить малый и средний бизнес;
- Утечка информации и репутационные риск для компании;
- **Анализ защищённости – страховка Вашего бизнеса.**

Что говорит закон?

Приказ ФСТЭК России № 17

П. 16. Внедрение системы защиты информации информационной системы включает:

Анализ уязвимостей информационной системы → принятие мер защиты информации по их устранению

Приказ ФСТЭК России о КИИ

13.6. в) Выявление уязвимостей

13.6. д) Тестирование на проникновение

Анализ защищенности от SaveIT Group

Анализ уязвимостей	Выявление уязвимостей	Тестирование на проникновение

Best Practice

ISO 27001 Certified · PCI DSS Compliant · ITIL® · NIST National Institute of Standards and Technology · OWASP Open Web Application Security Project

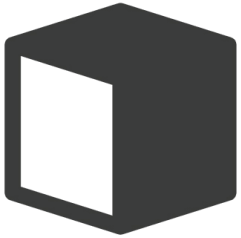
OSSTMM · ISF Standard of Good Practice for Information Security · ISSAF Information Systems Security Assessment Framework www.oissg.org · Penetration Testing Execution Standard · ISO 20000 · COBIT 5 An ISACA® Framework

Уровень осведомлённости аудитора о внутреннем устройстве системы

Black Box («Чёрный ящик»)
– максимально приближен к реальной ситуации,
– не предоставляются данные об объекте (защитных средствах, ИТ/ИБ персонале),
– используются только общедоступная информация об объекте атаки,
– аудиторы выступают в роли внешнего нарушителя.

Gray Box («Серый ящик»)
– в наличии определенный, небольшой, объем информации об атакуемом объекте (средства безопасности, операционные системы, информация о сетевом оборудовании, идентификаторы точек беспроводного доступа, IP- адреса),
– аудитор может иметь доступ к внутренней сети (низкий уровень прав доступа).

White Box («Белый ящик»)
– используется вся информацию о внутренней структуре/ реализации/устройстве объекта тестирования,
– аудитор выступает в роли внутреннего нарушителя.



Каким способом аудитор взаимодействует с заказчиком

Black Hat («Чёрная шляпа»)

– полностью имитируются действия злоумышленника,
– о проведении работ знают только руководители службы ИБ,
– проверка уровеня оперативной готовности к атакам сетевых администраторов и администраторов ИБ.

White Hat («Белая шляпа»)

– основная задача - обнаружение возможных уязвимостей и оценке риска проникновения в систему,
– меры по сокрытию атакующих действий не применяется,
– Аудиторы работают в постоянном контакте с ИБ-службой заказчика.

Методики анализа защищенности от SaveIT Group

- **Аудит исходного кода** на наличие уязвимостей с использованием специализированного программного обеспечения;
- **Обратная разработка** с целью восстановления алгоритмов работы программы и последующим поиском уязвимостей;
- Активное и пассивное **сканирование сервисов и служб** с целью выявления уязвимостей, находящихся в открытом доступе (эксплоитов);
- **«Фаззинг»** — с целью выявления некорректной работы алгоритмов программ или протоколов взаимодействия, которые могут впоследствии являться векторами для создания 0day уязвимостей;
- **Аудит соответствия** — аудит конфигураций и сред функционирования с целью оценки соответствия выполнения требований регламентирующих нормативно правовых актов.

Методики анализа защищенности от SaveIT Group

- **Нагрузочное (стресс) тестирование** — тестирование производительности приложения, сервиса или протокола взаимодействия с целью определения уровня критической нагрузки (входных данных), после которого объект исследования перейдёт в состояние «отказ в обслуживании»;
- **Аудит социотехническими методами** — метод аудита защищенности организации, в ходе которого используются приёмы социальной инженерии, основанные на особенностях психологии людей: фишинг, претекстинг, кви про кво, дорожное яблоко, обратная социальная инженерия и некоторые другие;
- **Компьютерная криминалистика (форензика)** — комплекс мер для расследования внутрикорпоративных преступлений и случаев мошенничества, поиска уязвимостей и других инцидентов в сетевой инфраструктуре организации.

Отчёт по итогам проведения анализа защищенности от SaveIT Group

Результатами проведения анализа защищенности служит отчёт, который содержит:

- Цели и границы проведения анализа защищенности;
- Перечень используемых методик;
- Используемые режимы и сценарии проведения анализа защищенности;
- Выявленные уязвимости;
- Подробные инструкции по устранению, выявленных в ходе анализа защищенности, уязвимостей, а также рекомендации по модернизации имеющейся системы защиты информации.

Наименование уязвимости	Необходимые меры ЗИ
CVE-2017-0144 (Eternal Blue) Уязвимость протокола SMB	Установка последних обновлений Microsoft и выполнение указаний бюллетени безопасности MS17-010
CVE-2009-3103 (Negotiate Func Index) Уязвимость протокола SMB	Установка последних обновлений Microsoft и выполнение указаний бюллетени безопасности MS09-050
CVE-2008-4250 Уязвимость в NetAPI32.dll	Установка последних обновлений Microsoft
CVE-2003-0352 (RPC DCOM Overflow) Уязвимость в сервисе RPCSS	Ус
CVE-2003-0812 (NetAPI32.dll Overflow) Уязвимость в NetAPI32.dll	Ус

Рейтинг уязвимых служб/ПО

задача	Имя	узел	интер
Сканирование веб-ресурсов	80/TCP - HTTP	10.1.1.200	
Сканирование веб-ресурсов	443/TCP - HTTP SSL	10.1.1.170	
Сканирование веб-ресурсов	80/TCP - HTTP	10.1.1.180	29
Сканирование веб-ресурсов	80/TCP - HTTP	10.1.1.201	28
Сканирование веб-ресурсов	443/TCP - HTTP SSL	10.1.1.180	16
Сканирование веб-ресурсов	nginx Версия: 1.6.2	10.1.1.201	4

Диаграмма распределения уязвимостей по уровням риска

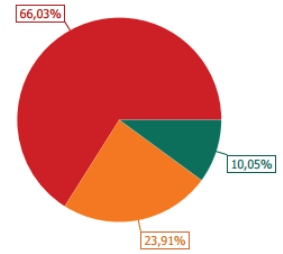


Таблица распределения уязвимостей по хостам

Хост / Риск	Высокий	Средний
192.168.8.151	147	126
192.168.8.13	42	23
192.168.8.19	1397	449
192.168.8.21	222	102
192.168.8.69	793	242
Всего	2601	942

Содержание

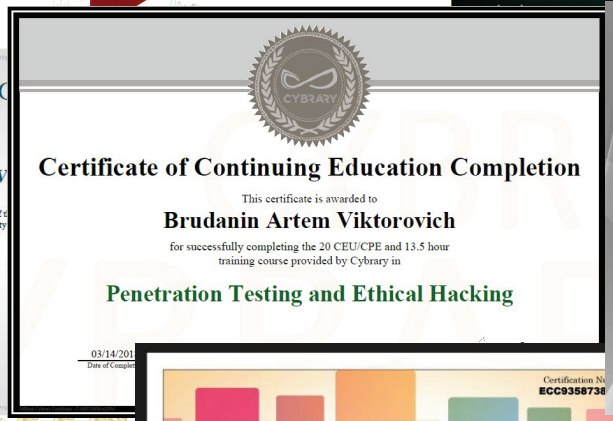
Рейтинг уязвимостей

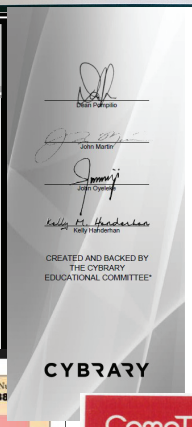
Уязвимость
Возможность межсайтовой подмены запросов
Внедрение произвольных команд
Возможность удаленного выполнения кода
Возможность перехвата сессии пользователя
Возможность внедрения SQL-кода
Список невидимых ссылок
Незащищенная передача данных
Возможна атака Anti DNS Pinning
Некорректный сертификат

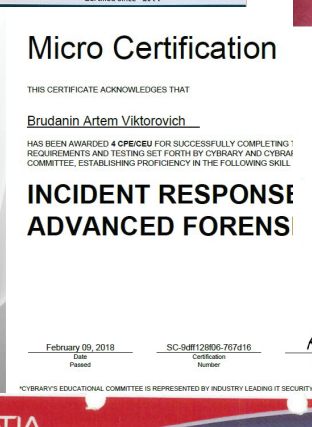
На сегодняшний день Анализа защищенности необходим каждой организации:

- Вы получите полноценную оценку текущего состояния информационной безопасности корпоративных ресурсов организации,
- Вы выявите существующие проблемы и выработаете эффективную систему обеспечения защиты информации,
- Вы минимизируете риски реализации угроз безопасности информационных ресурсов компании.

Команда профессионалов SaveIT Group







Опыт анализа защищенности от SaveIT Group

Правительство Воронежской области

Правительство Республики Крым

Министерство по развитию Дальнего Востока

Правительство Московской области

ГУП Московский метрополитен

ФКП Росреестра

Правительство Рязанской области

Администрация Нижнего Новгорода

Администрация Южно-Сахалинска

АО Конструкторское бюро химавтоматики

SAVE IT group

CyberSecurityRussia

Мы можем всё

Директор по развитию бизнеса SaveIT Group
Анна Попенко
+7 (930) 407-43-15 | popenko_a@saveit.pro

info@saveit.pro

+7 (800) 250-87-34