

Игра в рулетку, или Как выбирать средства защиты

Наталья Куканова

Positive Technologies

Ведущий эксперт

Образовательная программа «Практическая безопасность»

Что такое анализ рисков?

Выбор оптимального решения с учетом всех возможных факторов.

- Доделать всё сегодня или завтра прийти пораньше?
 - «Завтра приду пораньше, а сегодня вечером встречу с друзьями. С другой стороны, если я встречу с друзьями, то пораньше не приду...»
- Куда поехать в отпуск?
 - «Европа безопаснее, но зато Азия интереснее. А может, к маме в деревню? Там пирожки и варенье...»
- Проскочить на «светло-зелёный» или подождать зелёного?
 - «Везде успевает тот, кто никуда не торопится. Подожду зелёного...»
- Какой институт выбрать для ребенка?
 - «А может, пусть он сам себе институт выбирает?..»



Анализ рисков в ИБ

Цель – выбрать оптимальный набор средств защиты ИС.

Механизм – анализ рисков.

Важные факторы:

- ценность информации;
- угрозы и уязвимости ИС.



Идеальная картина. То, чего не может быть

- Методика анализа рисков определена и описана.
- Ценность данных определена.
- Угрозы и уязвимости выявлены.
- Риски определены и оценены.
- Средства защиты выбраны, приобретены, установлены и настроены.

Всё работает!



А в реальности...

- Владелец информации о ее ценности: «Ну, пишите второй уровень... Потому что он средний. А так вообще я не знаю, что писать».
- Поверхностный аудит выявил не более половины уязвимостей, а на кропотливый аудит не выделен бюджет.
- «Давайте везде поставим антивирусы и межсетевые экраны, потому что слова знакомые это важно».

Сложности

- Инвентаризация информационных ресурсов не проводится или проводится нерегулярно.
- Владельцам сложно определить ценность своей информации — даже при наличии методики.
- Кропотливый аудит, выявляющий большинство угроз и уязвимостей, требует значительного объема ресурсов.
- Регулярный процесс анализа рисков не поддерживается.

О чем мой рассказ

- Как определить уровень зрелости компании и зачем его определять?
- Почему важно не пытаться реализовать «классический» анализ рисков так, как написано в учебниках, если компания к этому не готова?
- Как найти максимально удобный механизм выбора мер защиты — вместо анализа рисков?

Модель зрелости



Модель зрелости согласно COBIT

№	Наименование	Состояние процессов управления рисками
0	Нулевой	Не применяются
1	Начальный	Процесс используется разово или в отдельных случаях и не организован
2	Повторяемый	Процесс повторяется по образцу
3	Определенный	Процесс документально оформлен и доведен до сведения участвующих сторон
4	Управляемый	Ведется мониторинг процесса в измеряемых показателях
5	Оптимизированный	Лучшие практики внедрены и автоматизированы

Подходы к определению средств защиты

Уровень зрелости	IT-процессы	Бизнес-процессы
Низкий (Base)	IT-процессы не построены. Все происходит «само собой» по инициативе отдельных сотрудников	Бизнес-процессы не формализованы. Владельцы процессов не назначены
Средний (Advanced)	Некоторые IT-процессы работают, но не документированы; нет мониторинга и контроля	Бизнес-процессы определены, но не классифицированы
Высокий (Risk Analysis)	Большинство процессов описаны и выполняются, организован контроль над их исполнением	Бизнес-процессы определены, описаны и классифицированы по степени важности

Подходы к определению средств защиты

Этапы оценки рисков \ Уровень зрелости	Низкий	Средний	Высокий
Инвентаризация ресурсов	+	+	+
Категорирование ресурсов		±	+
Определение угроз			+
Определение уязвимостей	+	+	+
Определение контрмер	+	+	+

Низкий уровень зрелости

- **Инвентаризация ресурсов:** узлы, ПО
- **Классификация** — только по инфраструктурному признаку:
 - Серверы, ключевые сетевые устройства (критичные)
 - Рабочие станции (некритичные)
- **Определение уязвимостей:** только критичные
- **Определение контрмер:** для критичных и некритичных ресурсов

Инвентаризация

Инвентаризация

Классификация

Определение уязвимостей

Определение контрмер

обнаружение узлов [Начало: 03.02.2012 17:47; Длительность: 2.16:13:32]

PenTest Сводная/узлы

Информация

id	IP-адрес	Имя в задаче	Имя NetBIOS	Имя FQDN	Операционная система
98	10.111.112.97	10.111.112.97	ACHERNOMOROV	ACHERNOMOROV	Microsoft Windows: Windows 7 Enter...
100	10.111.112.99	10.111.112.99		10.111.112.99	Microsoft Windows: Microsoft Window...
102	10.111.112.101	10.111.112.101		spatrol.ptsecurity.ru	Microsoft Windows: Windows Server ...
121	10.111.112.120	10.111.112.120	YMARYSHEV	ymaryshev.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
124	10.111.112.123	10.111.112.123	EKONOVALOV	ekonovalev.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
126	10.111.112.125	10.111.112.125	ASOZONTOV	asozontov.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
127	10.111.112.126	10.111.112.126	RLADUKHIN	rladukhin.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
129	10.111.112.128	10.111.112.128	VGERASIMOV	vgerasimov.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
130	10.111.112.129	10.111.112.129	YGOLTSEV	ygoltsev.ptsecurity.ru	Microsoft Windows: Windows 7 Ultima...
131	10.111.112.130	10.111.112.130	VZARICHNYY	vzarichnyy.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
134	10.111.112.133	10.111.112.133	AMIFTAKHOV	amiftakhov.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
135	10.111.112.134	10.111.112.134	ISCHERBININ	ischerbinin.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
139	10.111.112.138	10.111.112.138	DBELCHENKO-T...	dbelchenko-test.ptsec...	Microsoft Windows: Windows 7 Enter...
140	10.111.112.139	10.111.112.139	GGRITSAI	ggritsai.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
142	10.111.112.141	10.111.112.141	AZUIYKOVA	azuiykova.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
145	10.111.112.144	10.111.112.144	ANAVALKHIN	anavalkhin.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
147	10.111.112.146	10.111.112.146	AMOISEEV	amoiseev.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
158	10.111.112.157	10.111.112.157	OSHELESTOVA	oshelestova.ptsecurity...	Microsoft Windows: Windows 7 Enter...
159	10.111.112.158	10.111.112.158	DIVANOV	divanov.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
160	10.111.112.159	10.111.112.159	MKOSTANBAEVA	mkostanbaeva.ptsecur...	Microsoft Windows: Windows 7 Enter...
161	10.111.112.160	10.111.112.160	DGUTSKO	dgutsko.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
163	10.111.112.162	10.111.112.162	AERSHOV	aershov.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
164	10.111.112.163	10.111.112.163	SLAVRIKOV	slavrikov.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
176	10.111.112.175	10.111.112.175	DMAKRUSHIN	dmakrushin.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
190	10.111.112.189	10.111.112.189	SPOLONSKIY	spolonskiy.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
197	10.111.112.196	10.111.112.196	ENESTEROV	enesterov.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
209	10.111.112.208	10.111.112.208		testsurfpatrol.ptsecu...	Microsoft Windows: Microsoft Window...
210	10.111.112.209	10.111.112.209	TESTSURFPATROL	testsurfpatrol.ptsecu...	Microsoft Windows: Microsoft Window...
211	10.111.112.210	10.111.112.210	WIKI	wiki.ptsecurity.ru	Microsoft Windows: Windows Server ...
216	10.111.112.215	10.111.112.215	ACHAYKIN	achaykin.ptsecurity.ru	Microsoft Windows: Microsoft Window...
234	10.111.112.233	10.111.112.233	MKURSKIY	mkurskiy.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...
240	10.111.112.239	10.111.112.239	ASHISHKIN	ashishkin.ptsecurity.ru	Microsoft Windows: Windows 7 Enter...

Показывать информацию

Подробная информация

id 8
 IP-адрес 10.111.112.7
 Достоверность сканиро Службы не определены; все к...
 Имя FQDN 10.111.112.7
 Имя NetBIOS
 Имя в задаче 10.111.112.7
 Операционная система

Обнаружение ПО

Операционная система

Версия

Windows 7 Enterprise Service Pack 1 (x64) Метод определения: эвристический

Анализируемое ПО

Название	Версия	Путь
7-Zip	9.20	C:\Program Files\7-Zip
Firefox	8.0.1	
Google Chrome	18.0.1025.168	
IBM Lotus Notes	8.0.1	
Kaspersky Anti-Virus for Windows Workstations	6.0.4.1424	C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
MaxPatrol	8.23.1.12895	C:\Program files\Positive Technologies\MaxPatrol\
Microsoft .NET Framework	2.0 SP2	

Инвентаризация



Классификация



Определение уязвимостей



Определение контрмер

Классификация

Информация					
i	IP-адрес	Имя в задаче	Имя NetBI...	Имя FQDN	Операционная система
3	10.111.115.176	10.111.115.176	WIN7WMI	WIN7WMI	Microsoft Windows: Windows 7 Enterprise Service Pack 1 (x64)
2	10.111.113.197	10.111.113.197		10.111.113.197	Cisco IOS: 12.3(4)T2
4	10.111.115.172	10.111.115.172	DCA2008	DCA2008	Microsoft Windows: Windows 2008 R2 ServerEnterprise Service Pack 1 (x64)
1	10.111.115.175	10.111.115.175	WIN7_MP	WIN7_MP	Microsoft Windows: Windows 7 Enterprise Service Pack 1 (x64)

IP	NETBios	OS	Функция
1.1.1.1	nk	MS Windows 7	рабочая станция
1.1.1.2	es	MS Windows 7	рабочая станция
1.1.1.3	vk	RHEL	сервер
1.1.1.4	sd	RHEL	сервер
1.1.1.5	fg	HP-UX	сервер
1.1.1.6	bn	Cisco IOS	маршрутизатор
1.1.1.7	er	Cisco IOS	маршрутизатор



Обнаружение уязвимостей

445/TCP - Microsoft DS



Серьезная уязвимость

Обнаружен сетевой червь Conficker

ID: 8104

CVE: CVE-2008-4250

Краткое описание

Обнаружен сетевой червь Conficker, также известный как Downup, Downadup и Kido, который заражает компьютеры с операционной системой Windows.

Описание

Conficker (также известен как Downup, Do компьютерных червей, который впервые семейства Microsoft Windows (от Windows : вирус порастил 12 миллионов компьютеров Червь Conficker распространяется различн - использование уязвимости службы Serve сетевое соединение (RPC NULL session). У: - использование сетевых папок; Червь пь через сеть (используется словарь часто в - использование функциональных возможи Червь использует различные техники сам Помимо этого, он отключает в системе таи Центр обеспечения безопасности Window: сообщений об ошибках Windows (Windows антивирусов.

Решение

Для удаления программы воспользуйтесь

CVSS

Базовая оценка 10.0 (AV:N/AC:L/Au:N/C:AV:N данная уязвимость может эксплуат **AC:L** для эксплуатации уязвимости не тр **Au:N** для эксплуатации уязвимости прох **C:C** эксплуатация уязвимости влечет п **I:C** эксплуатация уязвимости влечет п **A:C** при успешной эксплуатации злоумь

Ссылки

<http://support.microsoft.com/kb/962007/ru>
<http://www.microsoft.com/technet/security/>
<http://iv.cs.uni-bonn.de/wg/cs/applications/>
<https://www.honeynet.org/node/389>

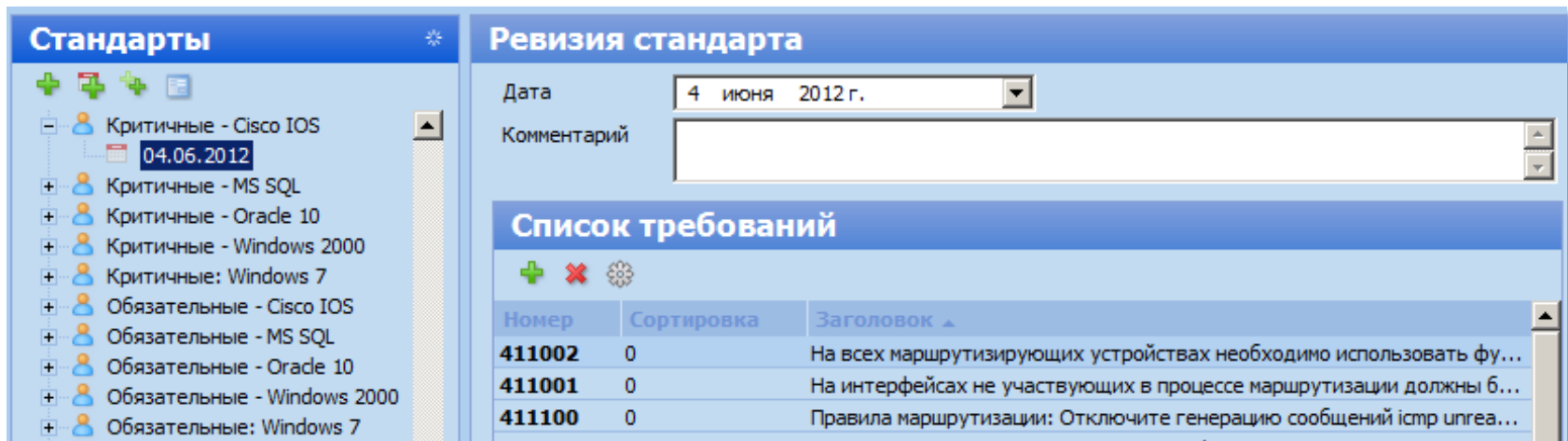
	Уязвимость	CVE	Количество
↑	Учетная запись пользователя		5
↑	Подобраны учетные записи		5
↑	Обнаружен сетевой червь Conficker	CVE-2008-4250	2
◇	Некорректный сертификат		6
◇	Некорректная цепочка сертификатов		6
◇	Подмена данных	CVE-2005-1794	5
◇	Виртуальная память не очищается		5
◇	Возможна атака Anti DNS Pinning		2
◇	Неавторизованный доступ	CVE-2009-3555	1
↓	Планировщик заданий		9



Выбор применимых требований

На основе лучших практик и экспертного мнения выбираются наборы требований:

- критичные – для важных инфраструктурных элементов;
- обязательные – для всех остальных.



Стандарты

- Критичные - Cisco IOS
- 04.06.2012
- Критичные - MS SQL
- Критичные - Oracle 10
- Критичные - Windows 2000
- Критичные: Windows 7
- Обязательные - Cisco IOS
- Обязательные - MS SQL
- Обязательные - Oracle 10
- Обязательные - Windows 2000
- Обязательные: Windows 7

Ревизия стандарта

Дата: 4 июня 2012 г.

Комментарий

Список требований

Номер	Сортировка	Заголовок
411002	0	На всех маршрутизирующих устройствах необходимо использовать фу...
411001	0	На интерфейсах не участвующих в процессе маршрутизации должны б...
411100	0	Правила маршрутизации: Отключите генерацию сообщений ismр unrea...

Результат

- Определены перечень узлов и установленное на них ПО.
- Узлы ранжированы по инфраструктурному признаку.
- Выявлены критичные уязвимости.
- Определены базовые перечни требований для критичных и некритичных ресурсов.

- Необходимо выявить, какие требования не выполняются,
— и приступить к их реализации.

Средний уровень зрелости

- **Инвентаризация ресурсов:** узлы, ПО, функции.
- **Классификация** — по инфраструктурному признаку и по принадлежности к бизнес-процессам:
 - критичным:
 - ключевые сетевые устройства;
 - ресурсы БП «Логистика»;
 - некритичным: например, серверы тестовых сред.
- **Определение уязвимостей:** высокая и средняя критичность.
- **Определение контрмер.**

Инвентаризация

IP	NETBios	FQDN	OS	Установленное ПО	БП	Функция
1.1.1.1	nk	nk.company.ru	MS Windows 7	MS Office Google Chrome Касперский ...	Бухгалтерия	рабочая станция
1.1.1.2	es	es.company.ru	MS Windows 7	MS Office ...	Аппарат генерального директора	рабочая станция

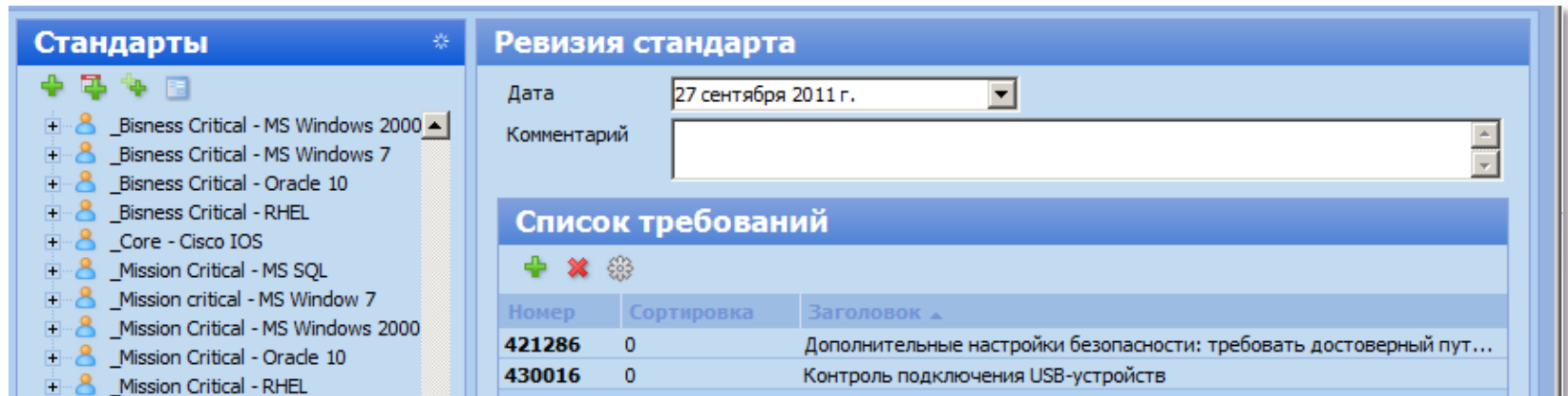


Классификация

Бизнес-процесс	Критичность	Уровень	Расшифровка
Логистика	1 ↑↑	1 ↑↑	Mission Critical
Продажи	1 ↑↑	2 ↑	Business Critical
Производство	1 ↑↑	3 ↑	Operations
Склад	1 ↑↑		
Аппарат ГД	2 ↑		
Бухгалтерия	2 ↑		
АХУ	3 ↑		

Выбор применимых требований

— Требования выбираются, исходя из уровня критичность бизнес-приложений, а также принадлежности к ключевой инфраструктуре компании

Стандарты

- + _Business Critical - MS Windows 2000
- + _Business Critical - MS Windows 7
- + _Business Critical - Oracle 10
- + _Business Critical - RHEL
- + _Core - Cisco IOS
- + _Mission Critical - MS SQL
- + _Mission critical - MS Window 7
- + _Mission Critical - MS Windows 2000
- + _Mission Critical - Oracle 10
- + _Mission Critical - RHEL

Ревизия стандарта

Дата: 27 сентября 2011 г.

Комментарий:

Список требований

Номер	Сортировка	Заголовок
421286	0	Дополнительные настройки безопасности: требовать достоверный пут...
430016	0	Контроль подключения USB-устройств

Результат

- Определены перечень узлов и установленное на них ПО.
- Узлы ранжированы по инфраструктурному признаку, а также по их принадлежности к бизнес-процессам.
- Выявлены уязвимости.
- Определены перечни требований для групп ресурсов.
- Необходимо выявить, какие требования не выполняются,
 - и приступить к их реализации.

Высокий уровень зрелости

- **Определить риски:**
 - определить активы компании и их владельцев;
 - определить угрозы, действующие на активы;
 - определить уязвимости, которые могут быть реализованы посредством угроз;
 - определить влияние нарушения конфиденциальности, целостности и доступности активов.
- **Проанализировать и оценить риски:**
 - оценить воздействие нарушения безопасности на бизнес-процессы компании;
 - оценить вероятность нарушения безопасности, учитывая доминирующие угрозы и уязвимости;
 - оценить уровень риска;
 - определить, является ли риск приемлемым или требует снижения;
- **Определить и оценить меры по снижению рисков. Возможные меры могут включать:**
 - применение необходимых мер и средств защиты;
 - разумное и объективное принятие рисков;
 - уклонение от рисков;
 - передачу соответствующих рисков третьей стороне.
- **Выбрать цели, меры и средства снижения рисков.**
- **Разработать план снижения рисков.**
- **Установить меры и средства снижения рисков.**



Заключение

- Для любого уровня зрелости компании существуют механизмы *осознанного* определения средств защиты. И это не всегда полноценный анализ рисков.
- Повышение уровня зрелости компании — в наших руках. Успешные методы управления информационной безопасностью неизбежно распространятся на всю компанию.



Конец рассказа Спасибо за внимание

Наталья Куканова

nkukanova@ptsecurity.ru