КАК ВЗЛАМЫВАЮТ ТЕЛЕКОМ:
РАССЛЕДОВАНИЕ РЕАЛЬНОГО ИНЦИДЕНТА

POSITIVE TECHNOLOGIES

Содержание

Недостаточная эффективность защиты корпоративной информационной инфраструктуры все еще остается актуальной проблемой. Крупные компании уделяют недостаточное внимание информационной безопасности на всех уровнях, как на уровне систем защиты, так и на уровне администрирования и мониторинга таких систем.

Анализ уязвимостей корпоративных информационных систем на протяжении нескольких предыдущих лет показывал наличие высокого процента информационных систем, имеющих те или иные уязвимости на внешнем периметре[1]. В 2016 году эти показатели сохранились. Так в 73% систем, в отношении которых был проведен внешний тест на проникновение, оказалось возможно преодоление внешнего периметра, а полный контроль над всей инфраструктурой организации был получен в 55% рассмотренных систем.

Рис. 1. Сложность преодоления периметра

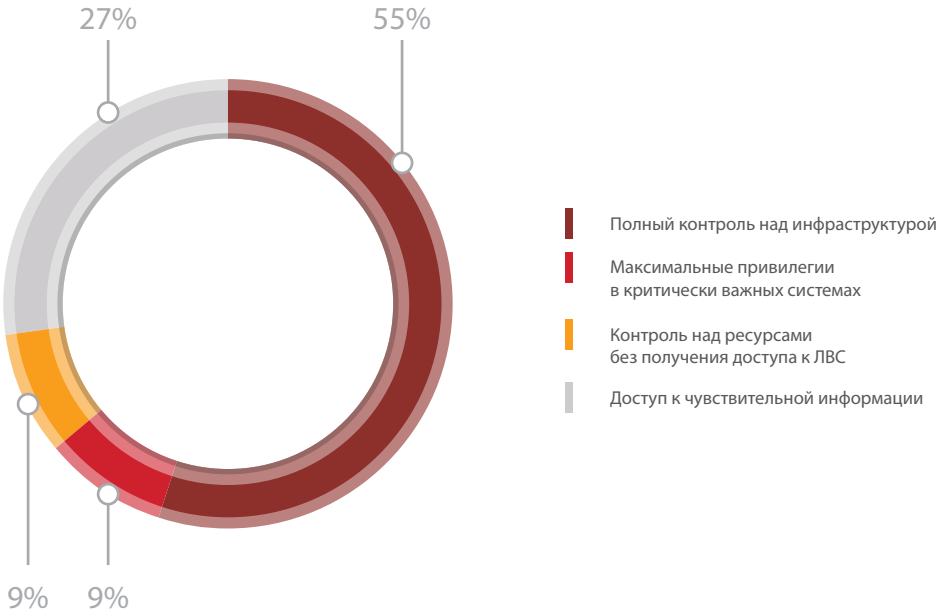

Рис. 2. Уровень привилегий, полученный от лица внешнего нарушителя

Эти результаты подтверждаются на практике. В рамках расследований реальных инцидентов ИБ выявляются артефакты, свидетельствующие о том, что злоумышленники зачастую используют для атак известные техники и эксплуатируют самые распространенные недостатки защиты и уязвимости систем. Пример одного из расследований компьютерного инцидента в крупной телекоммуникационной компании рассмотрен в данном отчете.

[1] http://www.ptsecurity.com/upload/ptru/analytics/Corporate-Vulnerability-2015-rus.pdf

Хронология атаки

Сетевые атаки на корпоративную инфраструктуру обычно проходят в два этапа, и данный инцидент не являлся исключением. Первый этап предполагает атаки на ресурсы сетевого периметра организации со стороны сети Интернет с целью получения доступа к ресурсам локальной сети, так называемое преодоление периметра сети, и второй этап — развитие атаки на ресурсы внутренней сети с целью закрепления в IT-инфраструктуре, получения полного контроля над ней и доступа к критически важной информации и системам. Данный отчет разделен соответственно на два основных блока, описывающих методы атаки, использованные нарушителем в рамках этих двух этапов.

Атака на сетевой периметр

Удаленная атака на любую корпоративную сеть начинается со сбора данных о сетевом периметре цели.

Предварительную информацию о сетевых узлах организации, доступных из Интернета, злоумышленник может получить, как от инсайдера, так и самостоятельно, собрав и проанализировав данные, доступные из открытых источников. Например, он может использовать следующие публичные сервисы для определения списка IP-адресов, имеющих отношение к сети организации:

- WHOIS-сервисы, предоставляющие возможность узнать регистрационные данные о владельцах доменных имен и IP-адресов;
- сервисы, предоставляющие возможность узнать содержание записей с DNS-сервера для указанного домена;
- NSLOOKUP-сервисы, предоставляющие возможность узнать содержание DNS-зоны домена по определенным типам записей;
- и другие.

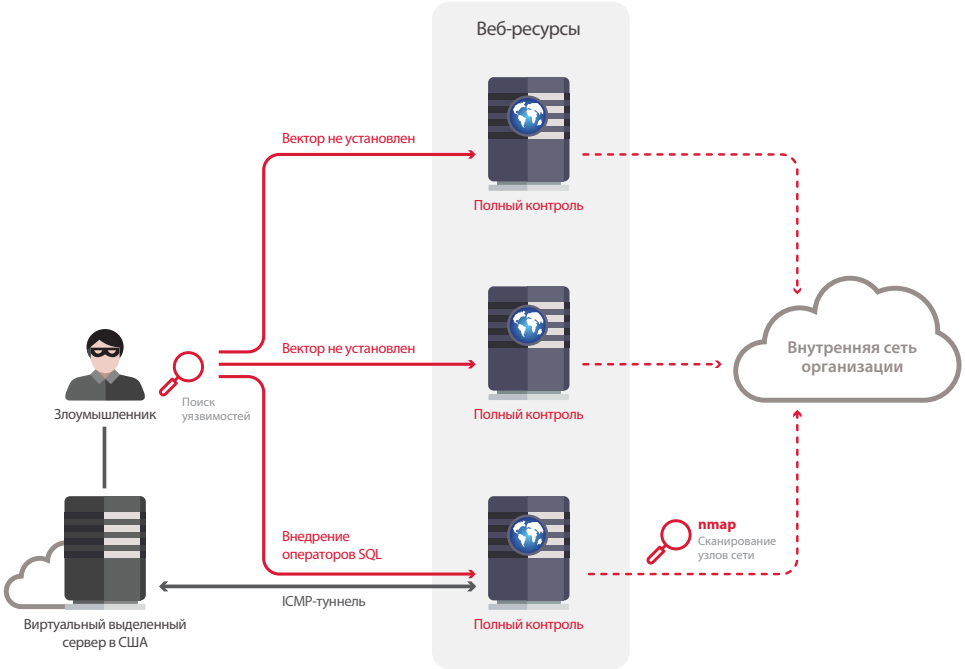

Рис. 3. Атака на внешний периметр

В первую очередь при инвентаризации ресурсов, принадлежащих жертве, злоумышленник определяет список публично доступных веб-ресурсов организации. В рассматриваемом сценарии преодоление сетевого периметра организации началось с выявления уязвимостей веб-приложений. Для упрощения и ускорения этого процесса был использован автоматизированный сканер.

Анализ журналов подключений на веб-серверах сетевого периметра показал, что сканирование велось в агрессивном режиме с использованием автоматизированного сканера уязвимостей Acunetix. Аномальный рост количества запросов к одному из веб-серверов свидетельствовал, что злоумышленник совершенно не скрывал факта сканирования. **Но, несмотря на такие неаккуратные действия со стороны нарушителя, атака оставалась незамеченной на протяжении месяцев!** Журналы событий содержали множество записей о подозрительных действиях, однако даже периодический их анализ не проводился. Если у пострадавшей организации был бы внедрен централизованный мониторинг с помощью системы корреляции и консолидации событий безопасности (SIEM), то служба безопасности своевременно получила бы уведомление о событиях, связанных с началом атаки, и смогла бы принять необходимые меры по предотвращению инцидента.

Примечательно, что во время одного сеанса сканирования у атакующего произошло изменение IP-адреса на адрес, относящийся к другому провайдеру. Это позволило предположить, что он мог использовать программный VPN-туннель, который был временно отключен. Именно такие события, зарегистрированные в журналах веб-сервера, позволяют устанавливать IP-адреса нарушителя, выдающие его реальное местоположение.

В результате сканирования атакующий обнаружил критически опасную уязвимость «Внедрение операторов SQL» в одном из веб-приложений. Внедрение операторов SQL является одним из распространенных способов атаки на веб-ресурсы, работающие с базами данных. Успешно проэксплуатировав найденную уязвимость, злоумышленник получил не только доступ с максимальными привилегиями к базе данных, хранящей учетные данные всех пользователей, в том числе администраторов ресурса, но и возможность выполнять команды на сервере с привилегиями СУБД. Поскольку данный веб-сервер был подключен к внутренней сети, то после получения контроля над ним у нарушителя появилась возможность доступа во внутреннюю сеть организации. **Для сетевого взаимодействия использовался созданный атакующим ICMP-туннель,** передающий данные на внешний виртуальный выделенный сервер, арендованный в США. Особенностью ICMP-туннеля является отсутствие необходимости использования транспортных протоколов, то есть ПО, обеспечивающее работу туннеля, не использует порты для передачи данных, а устанавливает логическое соединение с удаленным компьютером через эхо-запросы и ответы (ping), что позволяет обходить межсетевые экраны и оставаться необнаруженным.

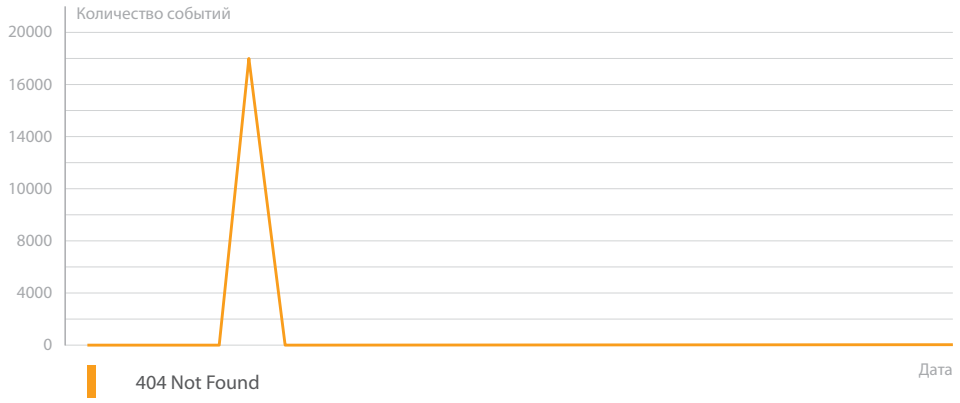

Рис. 4. Резко возросшее количество ошибок доступа к веб-приложению во время сканирования

Расследование инцидента показало, что всего было скомпрометировано три веб-сервера, к которым злоумышленник имел доступ с привилегиями локального администратора и использовал как точки входа во внутреннюю сеть организации.

Рис. 5. Объем журналов ошибок веб-сервера

Собранной с веб-серверов информации и результатов сканирования нарушителю было достаточно для того, чтобы продолжить успешно атаковать узлы внутренней сети.

Следует отметить, что атака на периметр сети организации прошла всего в два шага:

1. Автоматизированное сканирование с помощью сканера уязвимостей Acunetix.
2. Эксплуатация обнаруженной критически опасной уязвимости «Внедрение операторов SQL».

Исходя из этого, уровень защищенности периметра сети можно оценить как низкий. Подобная атака могла быть легко отражена еще на стадии проведения нарушителем разведки (поиска уязвимостей) межсетевым экраном уровня приложений (WAF), предназначенным для выявления и блокирования современных атак на веб-ресурсы. WAF позволяет блокировать попытки взлома и выявлять цепочки развития реальных атак, передавать информацию о произошедших событиях в систему SIEM для уведомления сотрудников службы безопасности и последующего оперативного реагирования.

Веб-приложения в основном используются как публичные ресурсы (официальный сайт, интернет-магазин, новостной портал и т. п.), доступ к ним должен быть обеспечен для любого пользователя сети Интернет. Это открывает нарушителю множество возможностей для осуществления атак. Например, критически опасная уязвимость в веб-приложении на сетевом периметре организации может позволить выполнять команды операционной системы на атакованном узле, что приведет к полной компрометации данных, расположенных на нем, и позволит злоумышленнику развивать атаки на внутреннюю сеть организации.

Закрепление в системе и развитие атаки во внутреннюю сеть

Получив доступ во внутреннюю сеть компании, злоумышленник со скомпрометированного сервера начал исследование ресурсов ЛВС. С помощью сетевого сканера Nmap он смог выявить на активных узлах открытые для подключения интерфейсы сетевых служб (TCP и UDP), определить по баннерам версии используемого ПО, а также определить потенциально уязвимые службы. Параллельно с этим процессом нарушитель отдельно осуществлял поиск веб-приложений, а некоторые ресурсы он исследовал вручную.

Проведенная инвентаризация ресурсов позволила нарушителю выявить доступные ресурсы и сделать предварительную оценку, какие из них наиболее перспективны для

развития атаки. В частности, в качестве следующей цели были выбраны терминальные серверы, предоставляющие пользователям организации вычислительные ресурсы для решения различных задач. Технология, на которой построен терминальный доступ, позволяет пользователям получать доступ к служебной информации с любого компьютера. При терминальном подключении создаются отдельные учетные записи пользователей, которые обеспечивают одновременную работу в единой операционной системе многих сотрудников. Однако из-за недостаточного уровня изоляции сессий пользователей компрометация одной учетной записи может повлечь компрометацию учетных записей других пользователей терминального сервера.

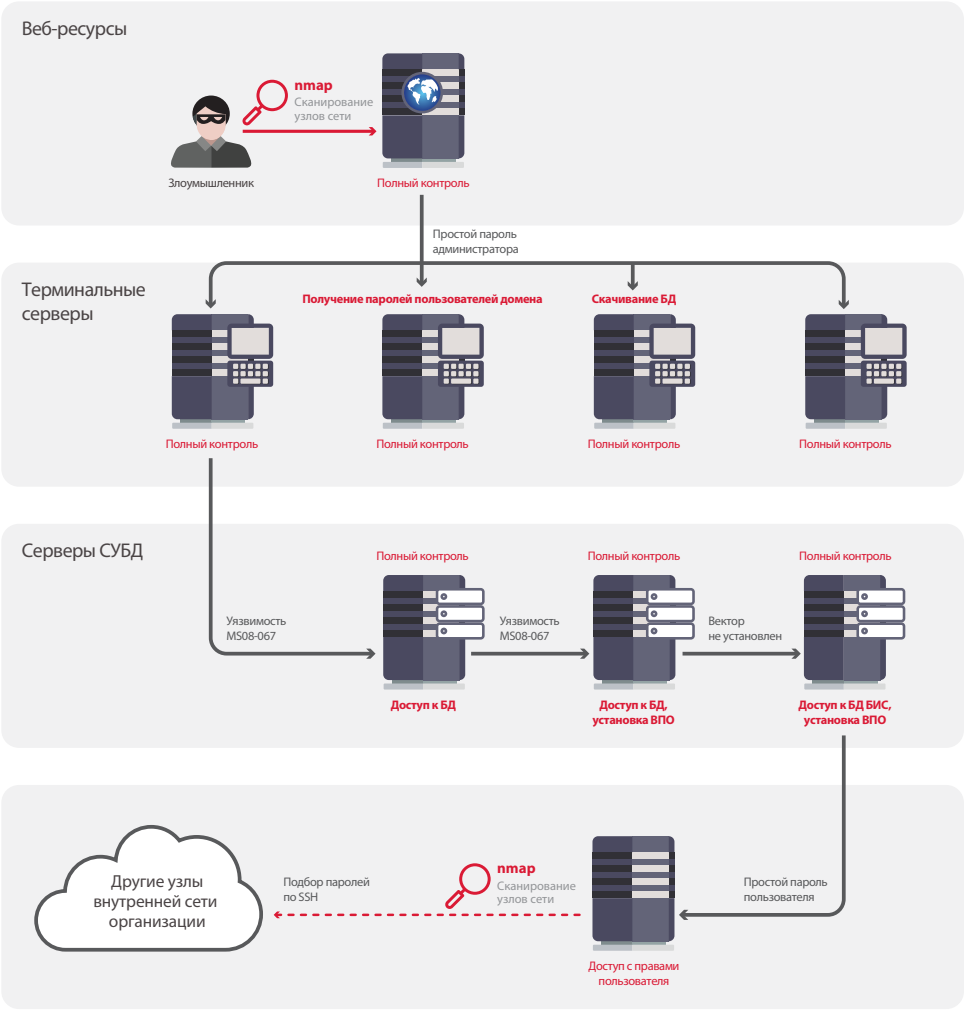

Рис. 6. Развитие атаки во внутреннем сегменте сети организации

В рассматриваемом инциденте по причине использования словарных паролей для учетных записей локальных администраторов злоумышленник легко получил привилегированный доступ сразу к нескольким терминальным серверам и затем скачал содержимое расположенных на них баз данных. На одном из серверов полученные привилегии позволили создать дамп памяти процесса lsass. Данному процессу соответствует сервис, который является частью операционной системы Windows, отвечающий за аутентификацию локальных пользователей отдельного компьютера. Из дампа памяти с помощью распространенной утилиты Mimikatz[2] было извлечено множество учетных данных (включая

[2] https://github.com/gentilkiwi/mimikatz

пароли в открытом виде) пользователей, которые проходили аутентификацию на этом сервере, в том числе привилегированных. Среди полученных данных присутствовали служебные учетные записи для поддержки терминальных серверов, а также различные учетные записи домена.

Полученный злоумышленником уровень привилегий позволил далее беспрепятственно развивать атаку с использованием учетных данных легитимных пользователей. Всего лишь за один месяц ему удалось своими действиями добиться компрометации множества ресурсов. Так, в ходе атаки была получена информация об идентификаторах и хешах паролей пользователей ОС Windows (базы данных SAM), данные о конфигурации и адресации сети, сведения об учетных записях пользователей, криптографические ключи базовых станций и другая информация.

Далее атака развивалась в направлении нескольких серверов, работающих под управлением устаревшей версии ОС Windows, на которых располагались базы данных и ресурсы биллинговой информационной системы (БИС). Для получения анонимного доступа с системными привилегиями к этим серверам злоумышленник воспользовался критически опасной уязвимостью MS08-067, сведения[3] о которой были опубликованы еще в 2008 году, тогда же был опубликован общедоступный эксплойт[4]. Серверы были полностью скомпрометированы, а содержимое баз данных похищено.

На один из этих серверов было установлено вредоносное ПО, не только блокирующее сообщения антивируса, но и обеспечивающее работу канала связи с командным сервером злоумышленника и позволяющее нарушителю удаленно управлять скомпрометированными серверами.

Обнаружение и расследование инцидента

Инцидент был выявлен, когда специалисты пострадавшей организации заметили зарегистрированные многочисленные попытки подбора учетных данных SSH для внутренних узлов со скомпрометированных серверов СУБД в выходные дни. Расследование проводилось в два этапа.

На первом этапе анализ инцидента проводился специалистами пострадавшей организации, однако расследование было затруднено тем, что регистрация событий велась в недостаточном объеме. За это время удалось выявить часть цепочки скомпрометированных серверов, определить узлы сети, с которых происходило развитие атаки, и обнаружить серверы, зараженные вредоносным ПО.

Ко второму этапу расследования были привлечены специалисты компании Positive Technologies. Как выяснилось в результате расследования, на момент начала этого этапа злоумышленник имел доступ ко внутренним узлам сети пострадавшей компании уже в течение 5 месяцев. После предварительного анализа данных об инциденте, полученных от пострадавшей организации, определены экстренные меры по минимизации рисков, такие как смена паролей для скомпрометированных учетных записей, выключение либо изоляция скомпрометированных объектов инфраструктуры. Это позволило перекрыть выявленные каналы взаимодействия нарушителя с узлами сети и остановить развитие атаки. В ходе углубленного анализа основного объема артефактов, выявленных на втором этапа расследования, было определено, что инцидент начался почти на месяц раньше той даты, которую удалось установить специалистам пострадавшей компании.

[3] https://technet.microsoft.com/ru-ru/library/security/ms08-067.aspx
[4] https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/sploits/6841.rar

Рис. 7. Сценарий развития атаки и этапы расследования инцидента

Анализ действий атакующего позволил сделать вывод о том, что злоумышленник являлся высококвалифицированным специалистом в области безопасности ОС, сетей, СУБД. Он был способен:

- оперативно выявлять и эксплуатировать уязвимости объектов инфраструктуры;
- закрепляться и оставлять альтернативные пути доступа к инфраструктуре;
- организовывать скрытые каналы передачи данных;
- извлекать и передавать критически важные данные на контролируемые им серверы в Интернете.

После того, как злоумышленник преодолел периметр сети организации, он не скрывал следы своего присутствия во внутренней сети и использовал распространенные средства инструментального сканирования в агрессивном режиме. Он мог решить, что система обнаружения атак и средства защиты работают неэффективно и не замечают его присутствия, поскольку он не был выявлен во время атаки на веб-серверы. Либо он точно знал, что такие системы защиты отсутствуют вовсе, основываясь, например, на результатах разведки.

У атакующего была техническая возможность перехвата учетных записей с паролями в открытом виде и доступа к технологическому оборудованию сотовой сети, установки закладок, триггеров, организации резервных каналов утечки информации и удаленного доступа к объектам инфраструктуры. Он мог свободно перемещаться по инфраструктуре, расширять привилегии и развивать атаку вплоть до установления полного контроля над доменами.

Выявление подобных действий на поздних этапах атаки крайне затруднительно в связи с использованием нарушителем учетных записей легитимных пользователей, применением вредоносного ПО, которое не обнаруживалось используемой в организации системой антивирусной защиты, а также в связи с коротким циклом перезаписи журналов событий и недостаточным их мониторингом.

Атака продолжалась до тех пор, пока все выявленные каналы взаимодействия с узлами в сети Интернет, с которых нарушителем производились несанкционированные действия, не были перекрыты. Однако это не исключает возможности сохранения у злоумышленника альтернативного доступа к сети.

Расследование показало, что в числе скомпрометированных ресурсов оказались:

- 3 узла на сетевом периметре;
- как минимум 4 терминальных сервера;
- серверы баз данных;
- множество учетных записей домена, в том числе служебные учетные записи для поддержки терминальных серверов с повышенными привилегиями;
- криптографические ключи базовых станций;
- множество других ресурсов во внутренних сетях, предположительно получен полный контроль над доменами.

Атака затронула ключевые подразделения организации, при этом с большой вероятностью были затронуты данные клиентов организации.

Выводы и рекомендации

В рассмотренном примере были продемонстрированы следующие основные недостатки в защите сетевой инфраструктуры организации, которые использовал атакующий и которые не позволили своевременно выявить и предотвратить инцидент:

+ недостаточно эффективный процесс выявления и блокирования современных атак на веб-приложения;
+ недостаточно эффективная реализация процесса регистрации событий безопасности и отсутствие выделенной системы сбора событий безопасности и мониторинга;
+ отсутствие сегментации сети;
+ отсутствие средств анализа сетевого трафика во внутренней сети организации;
+ слабая парольная политика и, как следствие, массовое использование словарных паролей учетных записей (как обычных пользователей, так и администраторов);
+ недостаточно эффективная антивирусная защита;
+ неустановленные обновления ПО на серверах инфраструктуры.

Анализ результатов расследования позволяет сделать вывод о том, что инцидента можно было вовсе избежать, если бы в пострадавшей организации были внедрены и интегрированы между собой SIEM-система, позволяющая организовать оперативный и ретроспективный мониторинг событий безопасности для выявления инцидентов на ранних стадиях, и WAF, своевременно выявляющий и блокирующий атаки на веб-ресурсы.

Кроме этого, следующие меры позволяют минимизировать риски подобных инцидентов в будущем:

+ регулярный анализ защищенности веб-приложений, своевременное устранение выявляемых уязвимостей;
+ реализация строгой парольной политики, запрещающей использование словарных и простых паролей, устанавливающей требования к длине, сложности и времени жизни паролей;
+ регулярный анализ защищенности ресурсов сетевого периметра с целью раннего выявления уязвимых узлов, а также возможных следов присутствия злоумышленников;
+ использование только актуальных версий ОС, ПО и антивирусных баз, обеспечение их регулярного обновления;
+ внедрение двухфакторной аутентификации для привилегированных учетных записей в критически важных системах и обеспечение принципа минимальных привилегий;
+ сегментация сети и строгое разграничение доступа между сегментами.

Таким образом, для повышения уровня защищенности и предотвращения подобных атак зачастую достаточно реализовать всем известные меры безопасности. Эти простые действия позволяют существенно усложнить задачу нарушителя, а применение эффективных систем защиты и мониторинга, проведение регулярных (например, дважды в год) тестов на проникновение позволяют свести вероятность взлома к минимуму.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

POSITIVE TECHNOLOGIES

ptsecurity.ru
pt@ptsecurity.com

facebook.com/PositiveTechnologies

facebook.com/PHDays