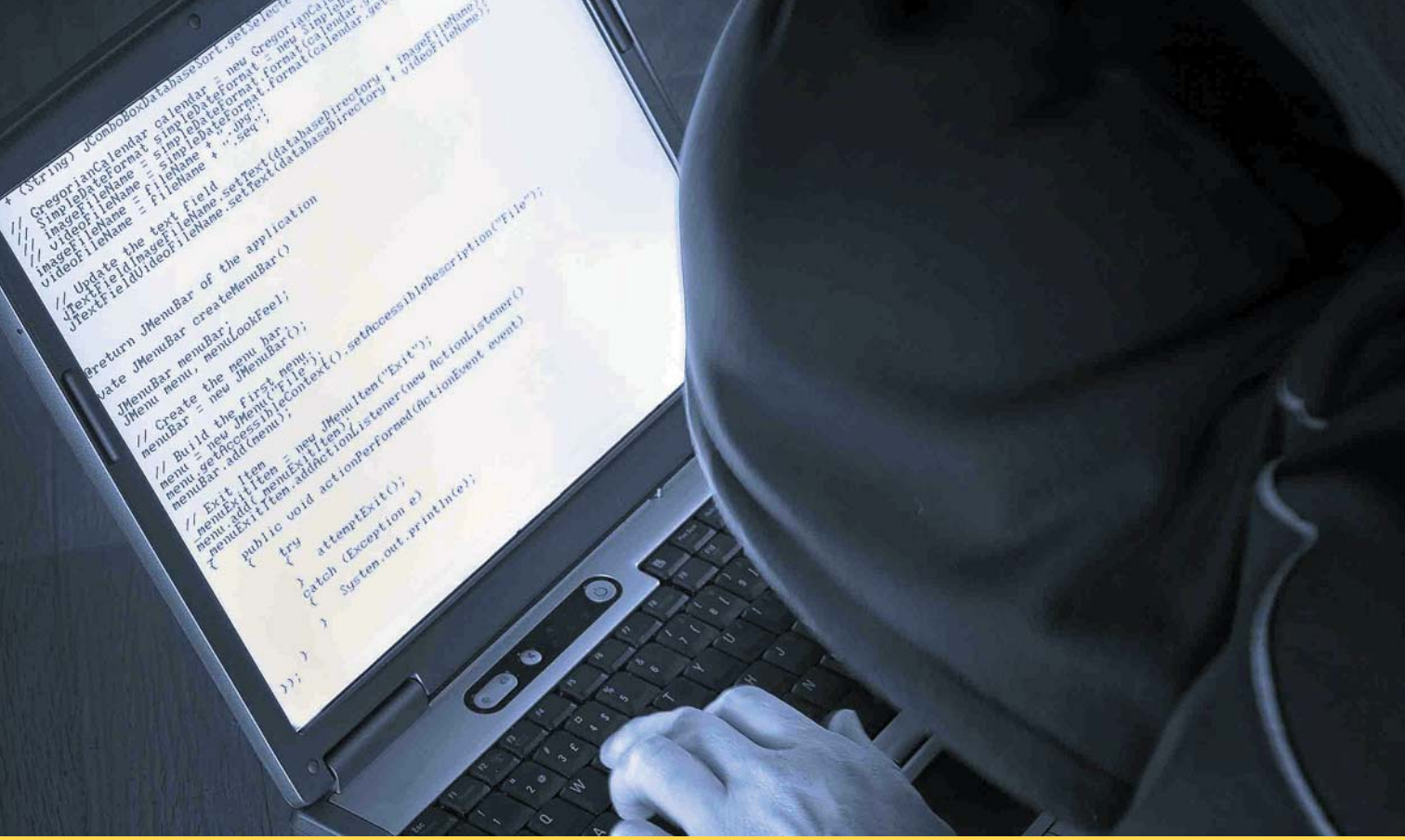

ХАКЕРСКИЕ АТАКИ НА СИСТЕМЫ УПРАВЛЕНИЯ В НЕФТЕГАЗОВОЙ ПРОМЫШЛЕННОСТИ: БУДЬТЕ ГОТОВЫ

КРИС ШИПП (CHRIS SHIPP)
ПЕРЕВОД: АЛЕКСЕЙ РЕВЕНКО

Удачные хакерские атаки на финансовые учреждения и коммерческие предприятия достаточно освещаются в прессе. Нынче даже самые технически грамотные пользователи, использующие Интернет для банковских расчетов и покупок, переживают за свою безопасность. Что уж тут говорить о нефтегазовой промышленности, в которой атаки на системы наблюдения и управления процессами добычи, хранения и транспорта газа и нефтепродуктов могут повлечь за собой фатальные последствия. Эту опасность необходимо осознавать на всех уровнях данной отрасли.

Бывший разработчик компьютерных игр Дэн Кауфман (Dan Kaufman), а ныне сотрудник Департамента обороны США, занимающийся интернет-безопасностью, 8 февраля 2015 г. продемонстрировал, как, используя систему встроенной экстренной связи, взять под контроль компьютерную систему автомобиля, чтобы получить полный контроль над ускорением, торможением и даже клаксоном. Это и другие последние разоблачения дали совершенно ясно понять, что современная компьютерная безопасность не менее важна, чем защита банковского счета. На сегодня важнейшими являются вопросы защиты каждого подключения к Интернету, включая системы контроля и управления — системы, которые управляют буквально всем: от производства каждого отдельного продукта до дамбы Гувера, а также как промышленные, так и домашние системы климат-контроля.

ОСОЗНАНИЕ ОПАСНОСТИ

Большинство из нас вряд ли осведомлены о постоянных атаках на системы контроля, управляющие почти всеми процессами производства, технологическими и торговыми операциями. Однако такие системы также используются в нефтегазовой промышленности для наблюдения и управления процессами добычи, хранения, транспорта газа и нефтепродуктов, и в последнее время было совершено множество кибератак на них, причем некоторые повлекли за собой катастрофические последствия. В частности, в свежем отчете Федерального управления по информационной безопасности Германии (Federal Office of Information Security) говорится: «На один из немецких сталелитейных заводов была совершена кибератака. Хакеры получили доступ к производственным сетям, что позволило им изменять настройки доменной печи». Сам факт того, что хакеры получили доступ к управлению доменной печью на сталелитейном заводе, может показаться удивительным. Однако некоторые люди, работающие в данной отрасли, утверждают, что киберзащита систем контроля в этой области — бессмысленная трата времени и ресурсов. Более того, часто говорят, что киберзащита даже вредит системам управления, так как негативно сказывается на надежности их работы.

Такая точка зрения основана на изначально неверном суждении о том, что киберзащита не нужна в среде систем управления, так как такие системы независимы. Другими словами, если система не имеет выходов во внешнюю среду, то она не подвержена атакам извне. Эти суждения ошибочны по двум причинам:

- большинство систем управления имеют подключение к Интернету, пусть не напрямую, а через корпоративную сеть;
- даже те системы, которые в реальности не имеют подключения к Интернету, подвержены опасности (наиболее значимый пример — компьютерный червь Stuxnet).

Конечно, вы не обязаны знать о хакерской атаке на ядерный обогатительный комбинат в Иране в 2010 г. Тогда хакеры увеличили скорость вращения центрифуг до значений, лежащих за пределами их возможностей. В то же время операторы получали информацию, что центрифуги работают в штатном режиме. Многие считают, что «червь» отбросил ядерную программу Ирана на несколько лет назад. Важно отметить, что Stuxnet был запущен в систему, которая не имела никакого выхода во внешнюю сеть. Каким образом тогда вирус попал туда? Один из проверенных сотрудников принес USB-накопитель, зараженный Stuxnet, и подключил его к компьютеру во внутренней сети.

ПРИМЕРЫ АТАК

Интересным примером атак на системы управления является кампания, известная как Energetic Bear/Crouching Yeti («энергетический медведь»/«крадущийся йети»), потому что она демонстрирует, какие используются механизмы, а также — насколько часто такие кампании кибершпионажа стали иметь место. «Лаборатория Касперского» — «царица» российского антивирусного программного обеспечения — опубликовала отчет, в котором говорится, что злоумышленники, стоящие за Energetic Bear, успешно провели 2800 кибератак, включая более 100 атак на корпорации в США, Японии, Германии, Франции, Италии, Испании, Турции, Ирландии и Китае. В начале своей деятельности Energetic Bear атаковали всех подряд, но исследователи из Symantec обнаружили, что с марта 2014 г. целью кампании стали предприятия энергетической промышленности.

Более того, специалисты Symantec заявляют, что атаки Energetic Bear на системы управления были настолько успешны, что «могли бы нанести ущерб или сорвать поставки энергии в подвергшиеся атаке страны» и что в их цели входило нанесение вреда «операторам энергетических сетей, основным предприятиям энергодобывающей промышленности, операторам газотранспортных систем, а также производителям оборудования для систем управления, которое используется в энергетической промышленности».

МЕТОДИКИ АТАКИ

Как же у кибершпионов, особенно у тех, которые проводят кампанию Energetic Bear, получается так успешно захватить контроль над компьютерами множества различных корпораций, особо отдавая предпочтение системам управления? Конечно, хакеры, скорее всего, используют особо изощренные техники, которыми может управлять только элитная группа компьютерных гениев. Но тревожит то, что на самом деле все это весьма далеко от правды.

Улики указывают на то, что «наскоки» Energetic Bear проводились с использованием распространенных и легко исполнимых методов атак на всем известные слабые места систем управления. Во многих случаях хакеры использовали различные варианты «трояна» Havex Trojan — хорошо известного вредоносного программного обеспечения. Также очень часто использовался Metaspoilt — свободный инструмент, который практически не требует навыков программирования.

Вредоносный код, который связывают с атаками Energetic Bear, был распространен с использованием нескольких основных методов, включающих целевой фишинг и waterholing-атаки[1], а также зараженные обновления для SCADA (Supervisory Control And Data Acquisition).

Целевой фишинг (Spear-phishing) — это процесс рассылки электронных писем по определенному списку адресатов, в котором содержится или ссылка на вредоносное приложение, или зараженное вложение. На первый взгляд это похоже на обычный спам, который все мы получаем каждый день. Главное отличие — эти электронные письма отправляются определенным людям, о которых хакеры хорошо осведомлены. Следовательно, письма составляются в такой манере, чтобы не быть похожими на обычный спам. Например, если я знаю, что вы собираетесь посетить конференцию на следующей неделе, я отправляю вам целевое фишинг-письмо, которое содержит информацию о конференции и вредоносную ссылку. При открытии с виду безопасной ссылки вы попадаете на вредоносный сайт, где ваш компьютер тут же загружает вредоносное программное обеспечение.

При атаках типа Watering hole хакеры взламывают веб-сайты, на которые часто заходит целевая группа. В случае с Energetic Bear хакеры просто заразили веб-сайты производителей систем контроля, с которых пользователи

[1] Watering hole. Это словосочетание переводится с английского как «водопой», но нередко используется и для обозначения питейных заведений с постоянным кругом клиентов. Суть подобных атак состоит в том, что злоумышленники заражают вредоносным ПО веб-сайты, часто посещаемые их потенциальными жертвами. Это могут быть сайты компаний-партнеров или подрядчиков, общественных организаций и даже правительственных учреждений.

скачивали системные обновления. Заменяя оригинальные обновления на копии, в которых содержался вредоносный код, хакеры сделали так, что их жертвы сами заразили свои системы. Обратите внимание, что эта техника срабатывает даже в том случае, если целевая система управления независима, т. е. внутренняя сеть не подключена к внешним сетям.

Описанные методологии атак совпадают с ежегодным отчетом по безопасности от компании Cisco. В нем говорится, что хакеры основательно сместили направление своих атак с серверов и операционных систем на обычных пользователей с их браузерами и электронной почтой.

ЗАЩИТА СИСТЕМ УПРАВЛЕНИЯ

Ошеломляющий успех атак кибершпионов не может не беспокоить. Что-то должно измениться, если мы хотим хорошо защитить системы управления в нефтегазовой промышленности. Есть такая поговорка: длинная дорога начинается с первого шага. Хорошая новость состоит в том, что корпорациям нужно предпринять всего лишь несколько важных шагов, чтобы обеспечить надежную безопасность своих систем управления от таких кибершпионов, как Energetic Bear.

Шаг 1: начинаем с подбора команды

Никакой бизнес не сможет стать успешным без менеджеров высшего звена. Зачастую сотрудники подразделений ИТ, стремясь получить необходимое финансирование и ресурсы, чтобы начать разработку надежной защиты систем управления предприятия, и пытаясь донести до высшего руководства необходимость кибербезопасности, злоупотребляют техническими терминами и компьютерными словечками. Однако самые успешные программы по кибербезопасности продвигаются благодаря тем людям, которые могут объяснить необходимость компьютерной безопасности с точки зрения бизнеса, поскольку они обеспечивают связь между принимающими решения бизнесменами и техническим персоналом.

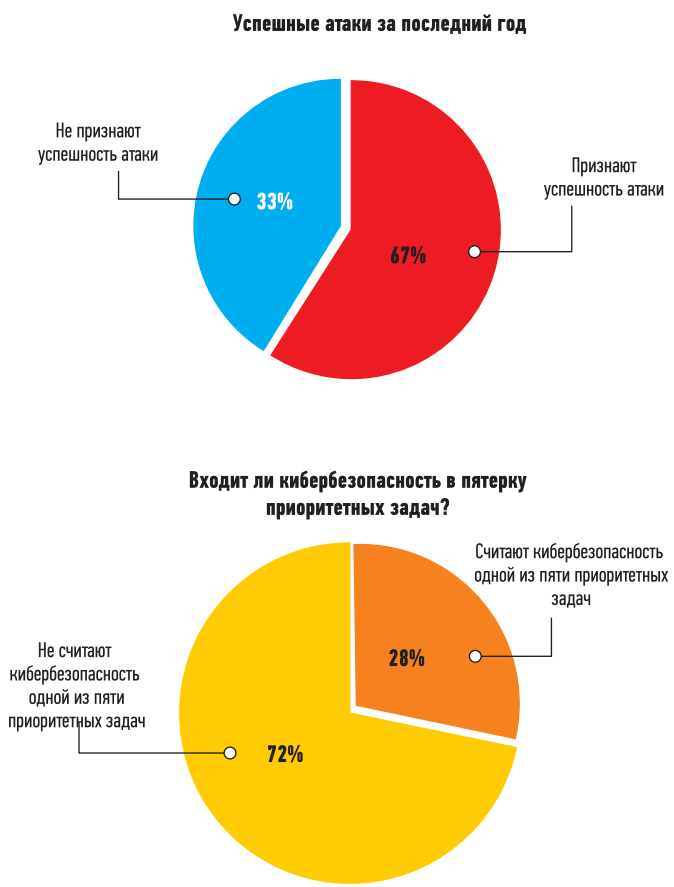

РИС. 1. ▶

Слишком часто компании переоценивают важность дорогого оборудования для сетевой безопасности — файерволов, систем обнаружения и защиты от атак и т. д., и недооценивают важность опытного и знающего технического персонала. У компаний, имеющих в штате постоянных сотрудников по сетевой безопасности со специальными знаниями и опытом, значительно лучше налажена защита данных, чем у компаний, которые тратят ресурсы на дорогое оборудование, но не имеют в штате хороших технических специалистов. Однако не каждый малый бизнес может себе позволить хорошего технического сотрудника. В этом случае стоит подумать об аутсорсинге вопросов, касающихся безопасности.

Шаг 2: используем эффективные методики

В июле 2014 г. Институт Понемона (*Ponemon Institute)* и Unisys выпустили отчет под названием «Критическая инфраструктура: готовность и уровень развития безопасности». В нем суммировались ответы 599 исполнительных директоров отделов безопасности из 13 стран, работающих в области нефтегазовой промышленности, альтернативной энергетики и перерабатывающей промышленности. 67% опрошенных указали, что за прошедший год их компании «как минимум один раз стали жертвой атаки, которая привела к потере конфиденциальной информации или привела к дестабилизации работы». Но в то же время всего 28% опрошенных считают кибербезопасность одной из пяти приоритетных задач бизнеса (рис. 1). Если члены высшего руководства прекрасно осведомлены об опасности, которой может подвергнуться их интеллектуальная собственность или даже производственные мощности, тогда почему они не считают ИТ-безопасность приоритетной задачей? Полагаю, дело в том, что большинство топ-менеджеров уже вложили много времени и ресурсов в ИТ-безопасность, но не получили требуемого результата. Следовательно, хоть они и осознают необходимость улучшения киберзащиты, они не видят возможности успешного решения проблемы и не уверены, что такое решение существует вообще.

Между тем существует прекрасное руководство по кибербезопасности для систем управления, которое мож-

но использовать независимо от уровня развития текущей программы по ИТ-защите. Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST) выложил в бесплатный доступ (http://nist.gov/cyberframework) «Концепцию по улучшению критической инфраструктуры кибербезопасности» (Framework for Improving Critical Infrastructure Cybersecurity). Этот документ представляет собой понятное практическое руководство для организаций, которые желают улучшить свои программы по кибербезопасности (рис. 2). Схожая волонтерская программа, известная как Critical Infrastructure Cyber Community («Критическая инфраструктура киберобщества»), или C-Cubed, также была сформирована на уровне Федерального правительства США для «поддержки промышленности в ее способности противостоять кибератакам».

Шаг 3: используем сбалансированный подход

В то время как большинство организаций нефтегазовой промышленности уже имеют налаженную систему кибербезопасности, многим еще предстоит развить достойную программу, которую будет поддерживать высшее руководство, в которой учтены известные концепции обеспечения безопасности, например предлагаемые NIST.

Довольно распространенная ошибка — сосредоточение максимума усилий и времени на предотвращении кибератаки. На первый взгляд это может показаться очевидной целью любой программы по киберзащите. Но тот факт, что самые успешные взломы не были обнаружены в течение 180 дней, заставляет нас изменить эту точку зрения.

Достоверно известно, что, несмотря на все усилия, компании нефтегазовой промышленности будут подвергаться атакам снова и снова. Но от чего зависит успех хакеров? Конечно, время от времени они будут получать доступ к вашим компьютерным системам. Однако если защиту строить на быстром обнаружении атак и устранении их последствий, ущерб будет минимальным. Таким образом, сбалансированный подход к обеспечению кибербезопасности значит, что мы должны посвящать столько же времени и усилий обнаружению и ответным действиям на атаку, сколько мы посвящаем предотвращению атак.

К сожалению, мало кто использует сбалансированный подход (рис. 3). Большинство компаний тратят очень много денег на предотвращение угроз (подготовку/защиту) и очень мало на обнаружение и ответные действия. Следовательно, если кибератака была проведена успешно, брешь в системе, скорее всего, не будет замечена еще весьма длительное время. А чем дольше хакеры остаются в среде незамеченными, тем большему риску подвержены эксплуатационные возможности организации. ⬣

СОВЕТЫ ПО ЗАЩИТЕ

- Смиритесь с тем, что ваши компьютерные системы в любом случае будут подвергаться атакам.
- Больше времени уделяйте тому, чтобы хакерам было трудно найти слабые места в ваших системах.
- Соблюдайте баланс в вашей программе кибербезопасности: убедитесь, что в ней заложены необходимые и достаточные возможности для обнаружения угроз и предусмотрены адекватные ответные действия на случай, если произойдет неизбежное.

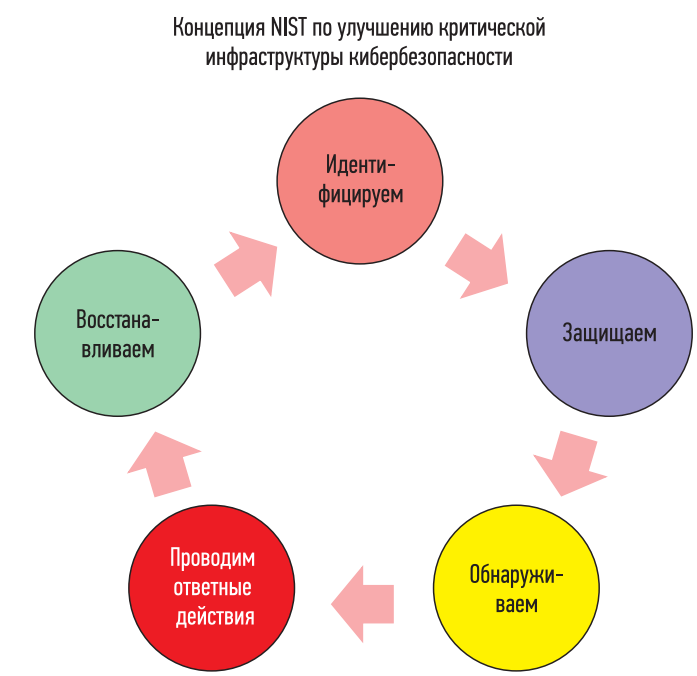

РИС. 2. ◀

Большинство компаний тратят очень много денег на предотвращение угроз... и очень мало на обнаружение и ответные действия

РИС. 3. ◀