Автор:
16.02.14 22:00 -

В США вышел перечень правил...

В США вышел перечень правил для улучшения информационной безопасности. 2 февраля Национальный институт стандартов и технологий США опубликовал первую версию “Фреймворка по улучшению информационной безопасности на уровне критической инфраструктуры”. Подготовка документа проходила совместно с Министерством внутренней безопасности. На протяжении года эксперты составляли список правил и стандартов для обнаружения рисков, а также дальнейшей защиты и восстановления системы. Данная версия руководства представляет собой ряд отраслевых стандартов и примеров их эксплуатации, которые могут быть полезны компаниям для более качественного обеспечения информационной безопасности.

Роскомнадзор потребовал заблокировать...

Роскомнадзор потребовал заблокировать два сайта с данными 10 тыс. россиян. Роскомнадзор потребовал заблокировать работу двух сайтов, которые нелегально распространяли личные данные россиян. Об этом сообщается на сайте ведомства. По утверждениям представителей Роскомнадзора доступ к ресурсам был ограничен регистратором доменных имен, который был зарегистрирован на территории Содружества Багамских островов.

Microsoft вступает в партнерство...

Microsoft вступает в партнерство для борьбы с киберпреступностью. Корпорация Microsoft анонсировала подписание трех новых глобальных партнерств с Организацией американских государств (the OAS), Европолом и FIS для расширения сотрудничества с международными правоохранительными органами и частным сектором в борьбе с киберпреступностью. Представители компании подписали меморандумы с тремя организациями во время первого ежегодного саммита Cybercrime Enforcement, в ходе которого приняли участие более 60 руководителей и специалистов правоохранительных органов и частного сектора для того, чтобы поделиться юридическими и техническими решениями для противостояния глобальному распространению киберпреступности в Сети.

Уязвимость в Magento...

Уязвимость в Magento позволяет раскрыть учетные данные пользователей. Как сообщают исследователи безопасности из компании Securatary, им удалось обнаружить опасную уязвимость в выкупленной eBay программной платформе Magento (используется в сфере электронной коммерции). Эксплуатация бреши позволяла раскрыть учетные данные произвольных пользователей, а также получить административный доступ к приложению. В настоящий момент уязвимость уже устранена.

Сноуден похитил пароль сотрудника...

Сноуден похитил пароль сотрудника для хищения секретных данных. Когда в Сети впервые появилась информация, рассекреченная бывшим сотрудником АНБ Эдвардом Сноуденом, правительство США заявило, что он незаконным образом получил доступ к данным. Тогда сообщалось, что бывший подрядчик ЦРУ похитил несколько паролей у своих сотрудников, правда, доказательств того предоставить никто не смог. Сейчас стало известно, что Сноуден действительно узнал пароль одного из работников АНБ, который затем использовал для извлечения секретных данных.

Anonymous опубликовали переписку Виталия Кличко.

Anonymous опубликовали переписку Виталия Кличко с советником президента Литвы. В четверг, 13 февраля, украинские активисты Anonymous заявили, что им удалось взломать электронный почтовый ящик советника президента Литвы Лауринаса Йонавичюса (Laurynas Jonavičius). По их словам, они получили доступ к переписке между литовским политиком и лидером украинской оппозиционной партии «УДАР» Виталием Кличко. «Содержимое этих писем показывает, как западные страны финансируют и контролируют Виталия Кличко при посредничестве литовского правительства», - заявили Anonymous.

Самокопирующегося червь.

Зафиксирована атака самокопирующегося червя на маршрутизаторы Linksys. Как сообщают исследователи из Sans, им удалось зафиксировать волну вредоносных атак, направленных на различные модели маршрутизаторов Linksys. Устройства инфицирует червь «TheMoon», главной особенностью которого является его способность самостоятельно распространяться.

В IE 10 обнаружена уязвимость нулевого дня.

Как сообщают эксперты безопасности из FireEye, им удалось обнаружить уязвимость нулевого дня (CVE-2014-0322) в web-обозревателе Internet Explorer. По их данным, в настоящий момент брешь активно эксплуатируется злоумышленниками. Это также подтвердили представители Microsoft.

Парламент ЕС отказал Сноудену в убежище.

Депутаты Европарламента отказались выполнять требования Европейской Партии Зеленых, которая призвала правительства стран ЕС предоставить убежище для бывшего сотрудника ЦРУ и Агентства национальной безопасности США (АНБ) Эдварда Сноудена. Данное решение было принято комитетом Европейского парламента по расследованию скандала, связанного с раскрытием шпионажа АНБ.

Anonymous организовали сбор средств...

Anonymous организовали сбор средств для одного из активистов. Группа активистов Anonymous в очередной раз решила «прийти на помощь нуждающимся». Так, на портале YouTube было размещено обращение к «жителям планеты», в котором Anonymous просят о помощи. Так, в обращении говорится, что один из операторов Anonymous в ближайшее время может оказаться на улице и прекратит поддержку микроблога @AnonymousPress в Twitter, у которого насчитывается более 100 тыс. подписчиков.

Хакеры похитили bitcoin...

Хакеры похитили bitcoin пользователей Silk Road 2 на сумму $2,747 млн. Как сообщило издание TechCrunch со ссылкой на модератора сайта Silk Road 2, известного как Defcon, хакеры осуществили атаку на ресурс и похитили 4474,26 монет bitcoin на сумму $2,747 млн. Вероятнее всего, злоумышленники эксплуатировали уязвимость в ПО для осуществления денежных операций с bitcoin и оплаты виртуальной валютой покупок на Silk Road 2.

ЕС не признал...

ЕС не признал публикацию ссылок на общедоступный контент пиратством. 13 февраля на официальном сайте Евросоюза появилась информация о том, что европейский суд принял решение отклонить иск по факту распространения ссылок на защищенный авторским правом контент, опубликованный в открытом доступе, и признать такие действия пиратством.

Уязвимости в домашних маршрутизаторах...

Уязвимости в домашних маршрутизаторах используются для компрометации банковских счетов. Как следует из сообщения исследователей безопасности CERT Polska, в ходе анализа хакерских атак с применением перехвата DNS они выяснили, что данные нападения зачастую становятся возможными благодаря уязвимостям в домашних маршрутизаторах. При этом целью злоумышленников, как правило, являются учетные записи пользователей банковских сервисов.

Во взломе Target применялись фишинговые атаки.

Как сообщает исследователь безопасности Брайан Кребс (Brian Krebs) со ссылкой на неназванные правительственные источники, взлому американской торговой сети Target предшествовала фишинговая атака на субподрядную компанию Fazio (сервис по обслуживанию отопительных и вентиляционных систем). По данным эксперта, злоумышленники присылали сотрудникам организации вредоносные письма, что в конечном счете позволило раскрыть учетные данные административной учетной записи в компьютерной сети Fazio.

Автор:
16.02.14 22:00 -

Read more http://www.linux-info.ru/obzor-korotkikh-novostej-s-10-02-14-po-16-02-14-g.html