Феміда на швидкості 150 км/год: чому в Україні статус нардепа став «ліцензією на вбивство»

Магічне зникнення підстав для санкцій проти резидента ФСБ Юрія Іванющенка

РПЦ як секта депортацій: свідчення Владислава Гаврилова про викрадення

Константин Корсун: «Существующая система кибербезопасности - живой труп»

КІБЕРЗЛОЧИННІСТЬ | СР, 2019-07-17 08:32

Версия для печати

«Основа национальной кибербезопасности - это хотя бы минимальное понимание и выполнение ее требований каждым гражданином Украины».

В издании "**Тиждень**" обсудили с директором компании Berezha Security Константином Корсуном необходимость кибергигиены, риски диджитализации Украины и проблемы с государственными органами кибербезопасности.

- Какие самые проблемные места сегодня в создании комплексной системы защиты информации (КСЗИ) на объектах критической инфраструктуры, которую предлагает Государственная служба специальной связи и защиты информации Украины (ГСССЗИ)?

- Дело в том, что после начала кибервойны в 2014-м и атаки вируса **NotPetya** в 2017

НОВИНИ

21:35 САП вимагає конфіскації майна у головного податківця Полтавщини

20:00 Погода в Україні на 8 травня: місцями короткочасні дощі та грози

19:09 Павло Казарін: Пастка безстроковості

18:04 Олег Чеславський: ЦПК і розкрадання стратегічних активів

17:10 Геннадій Левітас: Піхота - рід військ, який зникає

16:04 Касьянов: Вони крадуть 4 млн доларів на добу

15:10 Батьки очільника столичної прокуратури Сергія Ходаківського та судді Соборного суду Дніпра Максима Ходаківського у 2020 році придбали квартиру в Москві

14:59 ВАКС засудив заступника голови Рівненської облради за хабар до 9 років позбавлення волі

13:01 2500 гектарів лісу палає на Чернігівщині через російські обстріли

12:19 Підозрювана у хабарництві: ВРП звільнила львівську суддю Ірину Малех

ПІДПИСКА НА КАНАЛ

году Украина столкнулась с прогнозируемой, но для большинства неожиданной проблемой: почти на всех объектах критической инфраструктуры нет никакой защиты. Речь о государственных органах, водоснабжении, энергетике, пищевой промышленности, транспортной отрасли, банковском секторе, телекоммуникации и тому подобное. После последней мощной атаки прошло уже два года, тогда каждое четвертое украинское предприятие **попало под удар**, а общий ущерб от NotPetya в мире, по подсчетам американского правительства, превышают $10 млрд. Казалось бы, должны быть сделаны определенные выводы. Но, к сожалению, мы видим, что **это не так**.

> В тему: **82% програмного забезпечення в Україні не ліцензоване, — Business Software Alliance**

Предприятия или учреждения, которые начали подходить к вопросу киберзащиты серьезно, можно пересчитать по пальцам. Прежде всего это **Служба безопасности Украины** и Администрация президента (когда там работал Дмитрий Шимкив). СБУ занимается этим давно и целенаправленно, имеет довольно неплохой уровень, но это, так сказать, скальпель, спектр задач которого очень узок. Проблема в том, что очень многие **объекты критической инфраструктуры** принадлежат частному сектору. Вспомним то же Прикарпатьеоблэнерго, частную компанию, которая на тот момент просто не видела для себя рисков и не выделяла на это деньги. Насколько мне известно, сегодня вопросу киберзащиты очень большое внимание уделяет ДТЭК, а также ряд банковских учреждений и несколько IT-компаний.

За киберзащиту в стране отвечает ГСССЗИ. И ее отношение после атак никак не изменилось. Под давлением внешних партнеров Украины она смогла создать какие-то нормативные документы, например Закон «Об основных принципах обеспечения кибербезопасности», разработать стратегию. Формально на законодательном поле что-то делается, для западных партнеров достаточно слов «кибербезопасность» и «закон», а дальше уже никто не углубляется. В свое время я подробно изучил этот закон. Он кривой, коррупционный и ничего не решает, но дает дополнительные рычаги ГСССЗИ. А основной подход остается неизменным, речь идет о введении везде КСЗИ. Сама по себе идея неплохая, то есть у каждого объекта должна быть собственная **система защиты информации**.

- Почему она тогда не работает?

- Потому что идея устарела еще лет 10-15 назад. Люди, которые с этим сталкиваются, понимают, что это ни от чего не защищает, требует слишком много времени, усилий и средств. Это фактически расточительство, которое открывает широкое поле для злоупотреблений ГСССЗИ. Не может ни один стандарт четко определять, что нужно делать, это, скорее, определенный рамочный документ. Серия стандартов по киберзащиты ISO 2700 определяет общие требования, вместо того чтобы указывать, что именно надо сделать. Как и стандарт NIST (рекомендации по защите информации для предприятий США. - Ред.). Почему не может быть четких инструкций? Угрозы постоянно и очень быстро меняются. Зато украинский КСЗИ - это удивительная смесь рамочных определений и очень четких требований, которые не имеют отношения к современным вызовам. Но любая частная компания, например интернет-провайдер, предоставляющий информационные услуги и желающий работать с органами государственной власти, должен иметь у себя КСЗИ, якобы для того, чтобы защитить себя. В большинстве случаев это формальность, «бумажный тигр», который защищает разве что от проверок ГСССЗИ.

- Сколько компаний имеет такую КСЗИ?

- Насколько мне известно, около 17 провайдеров в Украине имеет у себя аттестованные КСЗИ. А в целом по стране их тысячи. Хотя само по себе требование по созданию КСЗИ незаконно, потому что оно основывается только на указе президента, а не на законе. При этом никто из бизнеса не хочет поднимать этот вопрос, подвергаться проблемы. А в недавние распоряжения, в частности в постановление Кабмина от 19 июля 2019 № 518 «Об утверждении Общих требований к киберзащиты объектов критической инфраструктуры», включено очень много коррупционных, принудительных и контрольно-надзорных положений.

- Почему, на ваш взгляд, возникают такие проблемы с ГСССЗИ?

- Служба является классической последовательницей советской административно-командной системы. Ведомство, которое является надзирателем с кнутом и которое может наказывать или миловать. Это создает пространство для коррупционных злоупотреблений. Хотя по уровню квалификации специалисты ГСССЗИ не выдерживают никакой критики. Молодежь, которая туда приходит, получает немного опыта, учится и очень быстро убегает, в основном из-за низкой зарплаты и плохой атмосферы. Поэтому я последовательно выступаю за ликвидацию этой структуры. Попробуем представить: а что произойдет, когда утром мы проснемся и узнаем, что ГСССЗИ ликвидирована? Учитывая обязанности этой службы, ничего плохого. Часть полезных функций вроде фельдъегерской почты или правительственной связи можно передать отдельным подразделениям или в МВД, или СБУ. С точки зрения кибербезопасности единственным полезным активом является CERT-UA. Это подразделение имеет достаточно опыта, в том числе взаимодействия с международными партнерами. CERT-UA знают как точку входа в страну, как доверенный контакт, к которому можно обратиться и получить квалифицированную помощь. Остальное в условиях гибридной войны никак не помогает, скорее, наоборот, мешает. Рынок услуг кибербезопасности без его регуляции прекрасно живет. Отдельная проблема - для ГСССЗИ не предусмотрена никакой ответственности. Если, например, на химическом заводе возникнет авария в результате кибератаки и окажется, что не было КСЗИ, за это накажут руководителя завода, а не ГСССЗИ. Даже сами представители Службы постоянно это подчеркивают.

Оставлять существующую систему кибербезопасности нецелесообразно. Это живой труп, там все сгнило, хотя он пытается кусать. Поэтому я за то, чтобы усыпить этого монстра, оставить только те вещи, которые еще можно и стоит реанимировать. У нас, кстати, уже был такой прецедент, ведь определенное время существовала

Государственная служба защиты персональных данных. Она должна была заниматься безопасностью этих данных, штрафовать предприятия, если они неправильно их хранили. Были очереди, ажиотаж, внимание прессы. А потом службу ликвидировали, и ничего в нашей жизни не изменилось, небо на землю не упало. Хотя, возможно, ее надо было бы оставить в ограниченной форме без карательных функций, чтобы она вела разъяснительную работу, рассматривала жалобы от потребителей. Такой прецедент следует повторить для ГСССЗИ, но с учетом ошибок.

- Однако возникает вопрос защиты критической инфраструктуры в условиях кибервойны. Как защититься и кто должен этим заниматься?

- Да, критикуя, предлагай. Я считаю целесообразным другой подход. Основа национальной кибербезопасности - это хотя бы минимальное понимание и выполнение ее требований каждым гражданином Украины. Как пользоваться смартфоном или интернетом, какие целесообразно использовать мессенджеры, какую почту можно открывать, а какую нет. Мы называем это кибергигиеной. Поэтому задача государства - максимально распространить соответствующие знания. На бордах, листовках, телефонной горячей линии, в учебных заведениях, на радио или телевидении. Государство должно помогать, а не контролировать. Единственная его функция, которая вообще востребована в этой сфере, - сервисная. Следующая задача - восстановление доверия к государству и его органам. Ключевым моментом национальной системы кибербезопасности является обмен информацией об инцидентах. Если произошла атака, допустим, на банк, он должен сообщить всем, как это произошло, все технические детали, чтобы остальные объекты смогли подготовиться. В большинстве случаев атаки типичны и устраиваются по очереди на всех объектах. Поэтому своевременный обмен информацией о таких инцидентах значительно снижает эффективность действий злоумышленников и масштабы ущерба. Но основывается он на доверии, ведь существуют риски разглашения чувствительной информации, которая может нанести репутационный ущерб. Особенно если речь идет о передаче сведений от частных структур к государственным. Нет доверия.

Я знаю несколько маленьких локальных примеров на уровне нескольких компаний, которые объединились и через доверенного провайдера создали собственную систему информирования о компьютерных инцидентах. Поэтому после первого шага, кибергигиены, нужен второй - создание организации, которая должна иметь высокий уровень репутации и доверия, с участием государства и иностранных партнеров. Команда специалистов должна получать рыночные зарплаты, деньги могут обеспечивать иностранные доноры. Первый год они должны давать абсолютно бесплатные рекомендации и помогать на всех уровнях, от простого до высокопрофессионального. Таким образом будет создаваться доверие. Конечно, этот процесс бесконечен, кто-то всегда будет сомневаться. Параллельно нужно создавать и развивать сеть обмена информацией, чтобы каждый ее участник не только принимал данные, но и предоставлял их сам. Это сложная, даже дипломатичная система, с ней надо обращаться очень осторожно. Зато сегодня закон требует, чтобы объекты критической инфраструктуры предоставляли данные об инцидентах. Это смешно, потому что они якобы должны, но им ничего не будет, если они откажутся или пришлют какую-то отписку. А чтобы проверить, нужны санкция суда на вмешательство в сеть и определенная квалификация, чтобы разобраться в деталях. Поэтому нельзя заставлять, человек сам должен понимать, что делиться надо.

- Готова ли Украина к повторению атаки уровня NotPetya? Удастся ли уменьшить убытки?

- Я думаю, уровень кибербезопасности не слишком изменился. Конечно, какие-то частные компании стали уделять этому вопросу больше внимания, больше учитывать безопасность. Но после атаки эта волна за полгода сошла практически на нет. Все движения в сторону кибербезопасности закончились. Таково свойство человеческой психики. Человек со временем привыкает к угрозе и перестает ее бояться. Поэтому на основе страха систему не построишь. Так что если россияне вдруг подумают, что сейчас подходящий момент для того, чтобы повторить атаку, убытки вряд ли будут меньше, разве что на 5-10%.

В тему: **Российские хакеры атаковали энергосети стран Балтии и Украины**

- Стоит ли ожидать таких атак в ближайшее время?

- Это неожиданность, которую невозможно предсказать. Перед президентскими выборами от киберполиции поступали предупреждения о вероятности атаки, но ее не было. Ничего масштабного не происходило уже более года. В то же время надо понимать, что кибератаки - это лишь дополнительный фактор дестабилизации наряду с проплаченными акциями протеста, провокациями на фронте, взрывами, убийствами или политическими демаршами. Задача кибератаки - усилить, помочь дезориентировать общество или направить его на свержение власти, референдум или приглашение вмешаться для соседней страны. Или другой вариант: атака на украинские энергетические системы состоялась сразу после отключения поставки электроэнергии в Крым, то есть некая месть. К тому же россияне любят устраивать атаки с определенным символическим значением. NotPetya был совершен в День Конституции Украины. Россияне знают наши слабые места, и если они захотят устроить атаку, особых трудностей у них не возникнет. Вопрос только в том, когда и почему они это захотят. Боты уже давно сидят во всех ключевых ведомствах. Усилий волонтеров для изменения нынешней ситуации недостаточно, надо принципиально все трансформировать.

- Кстати, об изменениях. Новый президент объявил курс на диджитализацию, переход к «государству в смартфоне». Это своевременно?

- Как человек, живущий в основном в цифровом мире, я не против, чтобы наше общество быстрее двигалось к уровню США или Европы. Но под диджитализацией понимается перевод в онлайн ряда бюрократических услуг, и это уже происходит. Те же центры предоставления административных услуг уже используют цифровые

решения. Они были созданы еще при предыдущем президенте, а начинались и сдвигались с мертвой точки при содействии западных партнеров, и этот процесс давно идет. Но если речь идет о каких-то чувствительных функциях, то надо внимательно разбираться. Например, я категорически против электронного голосования, поскольку оно не соответствует требованиям секретности. Невозможно проконтролировать, что человек делает выбор сознательно и без принуждения. Поэтому даже Эстония, известная своими успехами в создании электронного правительства, этого не сделала.

Если говорить о средствах идентификации, такие как BankID или MobileID, то там сразу возникает очень много вопросов по безопасности, в частности безопасности SIM-карты, потому что больше рисков связано именно с ее незащищенностью.

> В тему!: **Терабайты - «нефть» будущего. Метод анализа больших данных меняет социальную реальность**

Их, кстати, очень часто не принимают во внимание разработчики программного обеспечения. Большинство компаний, даже связанных с IT и довольно известные на международном рынке, о безопасности не имеют никакого представления. Часто это обусловлено банальным незнанием рисков и угроз. В регионах ситуация еще хуже, к сожалению. Там на некоторых предприятиях, заводах люди вообще не в курсе, что операционная система Windows XP уже давно не поддерживается. И мы не сможем приехать к каждому, нужна какая-то массовая коммуникация, на всю страну. Причем если в Киеве это можно распространить по каким-то цифровым каналам, даже через соцсети, то в регионах это, скорее всего, не сработает, поэтому необходимо искать креативные подходы.

Советы по кибербезопасности:

1. Иметь на компьютере и смартфоне антивирусное программное обеспечение, периодически обновлять его.

2. Для различных ресурсов использовать различные сложные пароли (электронная почта, соцсети и т.п.), периодически менять их. Не пользоваться генераторами паролей.

3. По возможности установить двухфакторную аутентификацию в соцсетях и сервисах.

4. Иметь резервную копию важной информации, сохранять ее без доступа к интернету.

5. Не открывать приложения к письмам от незнакомых адресатов, не переходить по ссылкам. А если от знакомых, то внимательно проверять перед открытием.

6. Не оставлять на ненадежных сайтах свои персональные данные (номер банковской карты и ее PIN-код, адрес электронной почты, номер телефона и т.д.), не сообщать эти данные по телефону.

7. Не отвечать на звонки с неизвестных номеров, особенно зарубежных. Не звонить на номера, указанные в смс-сообщениях о выигрыше призов, подозрительно больших распродажах или акциях.

8. Прежде чем посетить сайт или перейти по ссылке, удостовериться в надежности этого ресурса.

9. Не устанавливать программное обеспечение, в надежности или происхождении которого есть сомнения.

10. Осуществлять периодические платежи (коммунальные услуги, покупки в интернет-магазинах) только через надежные сервисы.

Константин Корсун родился в 1971 году. В 1993 году окончил Харьковское высшее военное авиационное инженерное училище и начал службу в СБУ. В 1996-м окончил Национальную академию СБУ. В 2000-м участвовал в создании первого подразделения противодействия компьютерной преступности в СБУ. С 2005-го по 2009-й служил в Департаменте безопасности информационно-телекоммуникационных систем ГСССЗИ, создавал CERT-UA и занимался его международной сертификацией. С 2009-го по 2014-й был руководителем украинского офиса компании iSIGHT Partners Europe. С 2014-го и до сих пор - соучредитель и исполнительный директор компании кибербезопасности Berezha Security&

—

Станислав Козлюк, фото автора; опубликовано в издании Тиждень

Перевод: Аргумент

В тему:

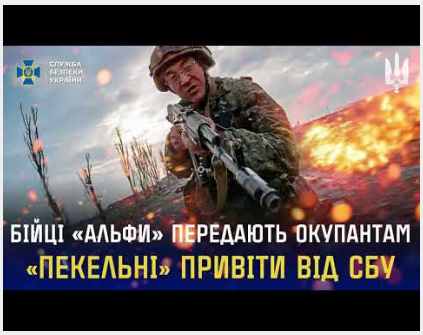
- **Увы, это не паранойя: за нами следят**
- **GDPR: мифы и реальность**
- **Как российские хакеры взламывали избирательную систему США. Секретный отчет АНБ**
- **«Антивирус Касперского»: угроза для государства Украина**
- **Битвы Великой технологической: как в современном мире сражаются за мировое господство**

Если вы заметили ошибку, выделите ее мышкой и нажмите ***Ctrl+Enter.***

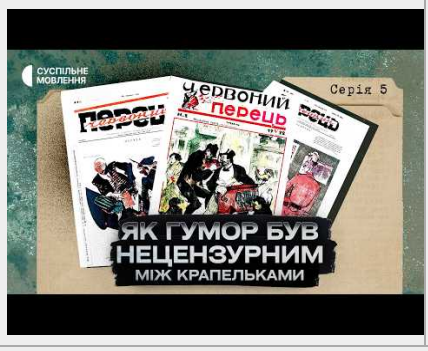
Коментарі

ВІДЕО

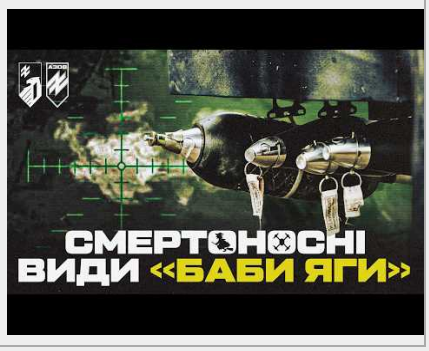
Воїни «Альфи» СБУ — ТОП-1 серед підрозділів Сил оборони за результатами бойової роботи у квітні



Про що не можна було жартувати в СРСР



HEAVY SHOT, VAMPIRE, NEMESIS: як «Баба Яга» б'є ок*пантів



Контакт: ***uargumentum@gmail.com***