CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 04.06.2020 г.

Съдържание

Нова платформа за тестване уменията на 6 най-търсени позиции в областта на киберсигурността

3 юни 2020 г.

Изграждането на екип за киберсигурност е необходимо на организации от всякакъв вид и размери. Това прави избора на подходящия човек за работата важна задача, при която тестването на знанията на кандидатите е основен компонент в процеса на наемане.

Обща практика е всяка организация да събере специален набор от въпроси за всяка роля.

Cynet стартира уебсайт за тестове за умения за киберсигурност, за да оптимизира процеса на наемане с автоматизирани онлайн въпросници за всяка позиция. Уебсайтът съдържа богат набор от въпроси за 6-те водещи позиции в киберсигурността, обхващащи всички аспекти на всяка от избраните роли.

Алгоритъмът за подбор включва 25 въпроса с повишаване на нивото на трудност.

Как работи платформата?

След създаването на акаунт в уебсайта за въпросници за киберсигурност, CISO - или всеки, който отговаря за наемането на специалисти по сигурността - може да вмъкне името и имейла на кандидата в интерфейса, а въпросникът ще бъде изпратен директно на кандидата.

Всеки кандидат трябва да отговори на всички 25 въпроса. След като кандидатът даде всички отговори, резултатите (както резултатът, така и времето, необходимо за отговорите) се показват на таблото за набор на служители.

Уебсайтът за тестове за умения за киберсигурност включва въпроси за следните позиции:

- **SOC Manager** - отговорен за установяването и надзора на работните процеси на мониторинг, управление и реакция на събития в сигурността, както и да гарантира спазването на SLA, придържането към процесите и импровизацията за постигане на оперативни цели.

- **SOC Analyst** - отговорен за първоначалния триаж на предупреждение, незабавно ограничаване, разследване, управление на действията по отстраняване и проактивно откриване на скрити заплахи.

- **Malware Analyst** - отговаря за изследване на открития зловреден софтуер чрез обратен инженеринг, статичен и динамичен анализ и др. Предоставя информация за характера на заплахите, които са насочени към организацията.

- **Security Architect** - отговаря за проектирането, изграждането, тестването и внедряването на системи за сигурност в ИТ мрежата на организацията, за да защити както бизнес данните, така и данните на клиентите.

- **IT Security** - отговаря както за ИТ, така и за основните политики и стандарти за киберсигурност. Тази позиция би била търсена оторганизации, които се нуждаят от умения за сигурност в своите екипи, но не могат да си позволят специална позиция за сигурност.

- **Incident Responder** - отговорен за пълния оперативен цикъл от първоначалното подозрение за нарушение и първите стъпки в разследването, през разкриване на обхвата и основната причина за инцидента до окончателни действия за отстраняване и възстановяване.

Ако имате кандидати за някоя от тези длъжности, просто създайте акаунт на уебсайта за тестове за умения за киберсигурност и започнете да тествате кандидатите.

За повече информация:

https://thehackernews.com/2020/06/cybersecurity-jobs-skill-testing.html

Firefox коригира изтичането на криптографски данни в най-новата си актуализация за сигурност

03 юни 2020 г.

Изминаха четири седмици от последната редовна актуализация за защита на Firefox.

Ако искате да проверите номерата на версиите си, Firefox 76.0 вече е заменен с 77.0; Firefox 68.8.0ESR вече е 68.9.0ESR, а браузърът Tor, базиран на Firefox ESR, вече е във версия 9.5 и базиран на 68.9.0ESR.

За организациите, ползващи Firefox, които са консервативни по отношение на новите функции на софтуера, но агресивни по отношение на инсталирането на пачове за сигурност, ESR версията е отличен компромис.

Списъците с грешки все още не са публични, вероятно за да се даде време на хората да инсталират актуализациите, преди те да бъдат използвани от недоброжелатели.

Какво да направите

Проверете дали имате актуализацията, като отидете на Help > About Firefox или на Help > About Tor Browser. (Използвайте елемента от менюто Firefox или Tor Browser вместо помощ, ако сте на Mac.)

Ако вече имате актуализацията, полето About ще ви каже; ако не, ще ви бъде предложено тя да бъде инсталирана.

Някои Linux и BSD дистрибутори са конфигурирани да доставят Firefox със собствен мениджър на пакети - ако вашият е един от тях, използвайте вместо това проверката за актуализация на операционната система.

За повече информация:

https://nakedsecurity.sophos.com/2020/06/03/firefox-fixes-cryptographic-data-leakage-in-latest-security-update/

Zoom не предлага шифроване „от край до край“ на безплатни потребители с цел подпомагане на правоприлагането

03 юни 2020 г.

Главният изпълнителен директор на Zoom разкри, че на потребители няма безплатно да се предлага криптиране „от край до край“, тъй като компанията иска да помага на ФБР и местните правоприлагащи органи при разследванията им.

Популярността на Zoom значително се увеличи от началото на пандемията COVID-19 поради многото хора, които са принудени да работят и учат от дома. Тази популярност привлече вниманието на експертите за поверителност и сигурност, които откриха някои сериозни проблеми в услугата за видеоконферентна връзка.

Zoom обеща да предприеме действия и вече започна да прилага мерки, които да му помогнат да се справи с проблемите със сигурността и поверителността.

Една от тези мерки е свързана с криптирането „от край до край“. Zoom криптира комуникациите между клиентите и неговите сървъри, но в момента не предлага истинско криптиране „от край до край“, което би попречило дори на самата компания да получи достъп до съдържанието на комуникациите на клиентите.

Миналия месец компанията публикува подробен проект на криптографския дизайн, който планира да използва за предстоящата си функция за криптиране „от край до край“, за който съобщи, че ще бъде предложен на плащащите клиенти и на училища.

Изпълнителният директор на Zoom Ерик Юан информира, че не искат да предлагат този вид защита безплатно на потребители, които са по-склонни да злоупотребяват с платформата, тъй като компанията иска да сътрудничи на ФБР и местните правоприлагащи органи, ако хората използват Zoom за „лоши цели“.От Zoom увериха, че не следят активно за съдържанието в платформата и не планират да го правят в бъдеще.

От Zoom обясниха, че ако е активирано шифроването „от край до край“, екипът на Zoom за доверие и безопасност няма да може да влезе в среща, за която смята, че е недобронамерена - и няма да има задна врата, за да се улесни такъв достъп. От компанията също отбелязаха, че някои функции за среща са несъвместими с криптирането от край до край. Ето защо то ще бъде включено „в обозримо бъдеще“.

За повече информация:

https://www.securityweek.com/zoom-not-offering-end-end-encryption-free-users-help-law-enforcement