EAGER7

Seven Steps To Full Control

EAGER7

Семь Шагов К Полному Контролю

LET`S GET STARTED!

Whether you are just starting your security journey or looking to take testing to the next level, securing your business is what we do, and we look forward to working with you.

НУ ЧТО? НАЧНЁМ!

Если вы только начинаете свой путь в сфере безопасности или хотите вывести тестирование на новый уровень, обращайтесь!

Обеспечение безопасности вашего бизнеса - это то, чем мы занимаемся, и мы будем рады сотрудничать с вами.

WHO ARE WE?

We are security professionals also known as ethical hackers, who use ethical hacking techniques to flesh out any security control weaknesses before someone with malicious intentions discovers them.

КТО МЫ?

Мы - профессионалы в области безопасности, также известные как этичные хакеры, которые используют методы этичного взлома, чтобы устранить все слабые места в системе контроля безопасности до того, как кто-то со злыми намерениями обнаружит их.

E7`S TESTING TEAM...

...has extensive experience conducting security testing and vulnerability assessments.

As a part of our penetration testing process, our knowledgeable security experts perform attack simulations and, in the process, uncover ways outsiders can try to gain access.

ПЕНТЕСТЕРЫ ИЗ E7

... имеют большой опыт проведения тестирования безопасности и оценки уязвимостей.

В рамках процесса тестирования на проникновение наши опытные эксперты по безопасности проводят имитацию атак и в процессе выявляют способы, с помощью которых посторонние могут попытаться получить доступ.

OUR AIM IS ...

...to find problems so you can put a stop to a security event before it starts and get full control over your cybersecurity.

НАША ЦЕЛЬ ...

...найти проблемы, чтобы вы могли предотвратить неприятные события, касающиеся безопасности вашей компании до того, как они произойдут.

Why Does My Business Need Penetration Testing?

Pentesting is a vital part of any business' cybersecurity strategy.

By identifying and fixing vulnerabilities before they can be exploited, you can reduce the risk of a data breach and protect your business from financial damages.

Почему моему бизнесу необходимо тестирование на проникновение?

Тестирование на проникновение является жизненно необходимой частью стратегии кибербезопасности любого предприятия.

Выявляя и устраняя уязвимости до того, как они могут быть использованы, вы можете снизить риск утечки данных и защитить свой бизнес от финансового и репутационного ущерба.

Benefits you'll derive from comprehensive security testing include:

- Identifying your vulnerabilities before cybercriminals do and plugging any security holes before a person with unlawful intentions finds them.
- Reducing your network downtime and avoiding the high costs of being offline for extended periods of time if a cyberattack were to occur.
- Preventing data breaches and financial losses due to system hacking.
- Ensuring your organization meets government and industry compliance rules.
- Building a solid reputation for your organization's adherence to security best practices.

Преимущества, которые вы получите от комплексного тестирования безопасности, включают:

- Выявление и исправление любых уязвимостей до того, как это сделают киберпреступники, или человек с противозаконными намерениями.
- Сокращение времени простоя вашей сети и избежание высоких затрат в случае кибератаки.
- Обеспечение соответствия вашей организации государственным и отраслевым нормам. Тестирование на проникновение требуется компания в соответствии с 683-П, 719-П, 757-П и ГОСТ 57580.
- Предотвращение утечек данных и финансовых потерь по причине взлома системы.
- Создание надежной репутации вашей организации, придерживающейся передовых методов обеспечения безопасности

WHY ARE CYBERSECURITY THREATS INCREASING?

Cybersecurity threats are increasing at an extraordinary rate, and so are the concerns of experiencing a breach. 68% of business leaders feel that their cybersecurity risks are increasing.

Software quickly becomes obsolete and not supported, and new patches are not provided to protect against newly found or created vulnerabilities.

Cyber threats also continue to evolve and appear in many forms, including phishing emails, phone calls or texts, malicious devices (i.e., USB drives), and exploiting system vulnerabilities.

Cybersecurity threats often mirror current events, which are also rapidly changing in today's world.

ПОЧЕМУ РАСТЕТ ЧИСЛО УГРОЗ В СФЕРЕ БЕЗОПАСНОСТИ?

Угрозы кибербезопасности растут с необычайной скоростью, как и опасения, связанные с их нарушением.

Программное обеспечение быстро устаревает и не поддерживается, а обновления не помогают для защиты от вновь найденных или созданных уязвимостей.

Киберугрозы также продолжают развиваться и проявляются в различных формах, включая фишинг, телефонные звонки или текстовые сообщения, вредоносные устройства (например, USB-накопители) и использование уязвимостей системы.

Угрозы кибербезопасности часто отражают

OUR SERVICES

PENETRATION TESTING:

BLACK BOX

GREY BOX

WHITE BOX

RED TEAM

ADVANCED PENETRATION TESTING

VULNERABILITY ASSESSMENT

МЫ ПРЕДЛАГАЕМ

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ (ПЕНТЕСТ):

BLACK BOX

GREY BOX

WHITE BOX

RED TEAM

РАСШИРЕННОЕ ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

АУДИТ БЕЗОПАСНОСТИ

PENETRATION TESTING

DEEP-DIVE, MANUAL PENETRATION TESTING PERFORMED BY EXPERIENCED AND CERTIFIED PENETRATION TESTERS.

BLACK BOX

This testing simulates the actions of an attacker as realistically as possible. We only know the name of the company and have a minimum of information.

GREY BOX

. Testers develop these simulations to understand issues that an average system could cause if they had bad intentions or if their login permissions were stolen. For example,
from rank-and-file employees.

WHITE BOX

This type of testing is used to check what damage can be done by attackers who gain access to administrator credentials. Tools of statistical and dynamic code analysis are used.

ПЕНТЕСТ

ГЛУБОКОЕ РУЧНОЕ ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ, ВЫПОЛНЯЕМОЕ опытными и сертифицированными специалистами.

BLACK BOX

Это тестирование максимально реалистично имитирует действия злоумышленника. Мы знаем только название компании и имеем минимум информации.

GREY BOX

Пентестеры разрабатывают такие симуляции, чтобы понять проблемы, которые могут возникнуть в обычной системе, если у пользователя будут плохие намерения, или если у него украдут права на вход в систему. Например, у рядовых сотрудников.

WHITE BOX

Этот вид тестирования используется, чтобы проверить, какой урон смогут нанести злоумышленники, получившие доступ к учетным данным администраторов. Используются средства статистического и динамического анализа кода.

RED TEAM

Multi-blended, adversarial-based attack simulation against people, software, hardware, and facilities performed simultaneously for the conservation of the target’s data security.

RED TEAM

Многокомпонентная имитация атаки на людей, программное и техническое обеспечение, оборудование и объекты, осуществляемая одновременно с целью сохранения безопасности данных объекта.

VULNERABILITY ASSESSMENT

A process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities of a system or systems. RedTeam Security will identify vulnerabilities within the in-scope systems, quantify their risk and prioritize them according to importance. Unlike a Penetration Test, these vulnerabilities will not be exploited.

A

аудит безопасности

И

ОЦЕНКА УЯЗВИМОСТЕЙ

Процесс выявления, количественной оценки и определения приоритетов (или ранжирования) уязвимостей системы или систем.

E7 выявит уязвимости в системах, входящих в сферу охвата, оценит их риск и расставит приоритеты по степени важности.

В отличие от теста на проникновение, эти уязвимости не будут использоваться.

ADMIN@EAGER7.NET

Thanks for your attention!

ADMIN@EAGER7.NET

Благодарим за внимание!