РЕШЕНИЯ ДЛЯ КИБЕРБЕЗОПАСНОСТИ

CYBER SECURITY SOLUTIONS

УДК 004.424

Камбулов Данил Александрович, магистрант, Донской государственный технический университет, г. Ростов-на-Дону

Kambulov D. A. kambulovdan@yandex.ru

Аннотация

Кибербезопасность - это практика защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от вредоносных атак. Он также известен как безопасность информационных технологий или электронная информационная безопасность. Этот термин применяется в различных контекстах, от бизнеса до мобильных вычислений, и может быть разделен на несколько общих категорий. Уровень киберугроз постоянно развивается и становится все более сложным, и большинство компаний не имеют собственных инструментов кибербезопасности и возможностей поддерживать меры безопасности в актуальном состоянии. Поскольку хакерам легче, чем когда-либо, инициировать атаку, организации теперь испытывают повышенный риск и более высокий уровень неопределенности. Впоследствии взломы и успешные атаки могут стоить компаниям миллионы, не говоря уже о вреде репутации бренда.

Annotation

Cybersecurity is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security or electronic information security. The term is used in

a variety of contexts, from business to mobile computing, and can be divided into several general categories.

The level of cyber threats is constantly evolving and becoming more complex, and most companies do not have their own cyber security tools and the ability to keep security measures up to date. Since it is easier than ever for hackers to initiate an attack, organizations now face increased risk and higher levels of uncertainty. Subsequently, hacks and successful attacks can cost companies millions, not to mention damage to brand reputation.

Ключевые слова: кибербезопасность, уровень киберугроз, решения по кибербезопасности, угроза, безопасность бизнеса, информационная безопасность.

Keywords: cybersecurity, level of cyberthreats, cybersecurity solutions, threat, business security, information security.

Решения по кибербезопасности — это инструменты, которые организации используют для защиты от угроз кибербезопасности, а также от случайных повреждений, физических бедствий и других угроз. Вот основные типы защитных решений:

Безопасность приложений - используется для тестирования уязвимостей программных приложений во время разработки и тестирования, а также для защиты приложений, работающих в производственной среде, от таких угроз, как сетевые атаки, использование уязвимостей программного обеспечения и атаки веб-приложений.

Сетевая безопасность - отслеживает сетевой трафик, выявляет потенциально вредоносный трафик и позволяет организациям блокировать, фильтровать или смягчать угрозы.

Облачная безопасность - реализует меры безопасности в общедоступных, частных и гибридных облачных средах, обнаруживая и исправляя ложные конфигурации безопасности и уязвимости.

Безопасность конечных точек - развертывается на конечных устройствах, таких как серверы и рабочие станции сотрудников, что позволяет предотвращать такие угрозы, как вредоносное ПО, несанкционированный доступ и использование уязвимостей операционной системы и браузера.

Безопасность Интернета вещей (IoT) - подключенные устройства часто используются для хранения конфиденциальных данных, но обычно не защищены конструктивно. Решения безопасности IoT помогают обеспечить прозрачность и повысить безопасность устройств IoT [1, 2].

Аналитика **угроз -** объединяет несколько каналов, содержащих данные о сигнатурах атак и субъектах угроз, обеспечивая дополнительный контекст для событий безопасности. Данные анализа угроз могут помочь службам безопасности обнаруживать атаки, понимать их и разрабатывать наиболее подходящие ответные меры [3].

Атака отказа в обслуживании

Отказ в обслуживании (DoS) атака перегружает целевую систему с большим объемом трафика, препятствуя способность системы нормально функционировать. Атака с участием нескольких устройств известна как атака распределенного отказа в обслуживании (DDoS) [4].

К методам DoS-атак относятся:

HTTP-флуд DDoS - злоумышленник использует HTTP-запросы, которые кажутся законными, для перегрузки приложения или веб-сервера. Этот метод не требует высокой пропускной способности или искаженных пакетов и обычно пытается заставить целевую систему выделять как можно больше ресурсов для каждого запроса.

SYN flood DDoS - инициирование последовательности подключения по протоколу управления передачей (TCP) включает отправку SYN-запроса, на который хост должен ответить SYN-ACK, который подтверждает запрос, а затем запрашивающая сторона должна ответить ACK. Злоумышленники могут использовать эту последовательность, связывая ресурсы сервера, отправляя SYN-запросы, но не отвечая на SYN-ACK от хоста.

UDP flood DDoS - на удаленный хост засыпается лавинная рассылка пакетов протокола пользовательских дейтаграмм (UDP), отправляемых на случайные порты. Этот метод заставляет хост искать приложения на затронутых портах и отвечать пакетами «Destination Unreachable», которые используют ресурсы хоста.

ICMP Flood - поток пакетов ICMP Echo Request переполняет цель, потребляя как входящую, так и исходящую полосу пропускания. Серверы могут пытаться ответить на каждый запрос пакетом эхо-ответа ICMP, но не успевают за скоростью запросов, поэтому система замедляется.

Усиление NTP - серверы Network Time Protocol (NTP) доступны для всех и могут быть использованы злоумышленником для отправки больших объемов UDP-трафика на целевой сервер. Это считается атакой с усилением из-за соотношения запросов и ответов от 1:20 до 1: 200, что позволяет злоумышленнику использовать открытые серверы NTP для выполнения крупномасштабных DDoS-атак с высокой пропускной способностью [5].

Инъекционные атаки

Атаки с использованием инъекций используют различные уязвимости для прямой вставки злонамеренных данных в код веб-приложения. Успешные атаки могут раскрыть конфиденциальную информацию, выполнить DoS-атаку или поставить под угрозу всю систему.

Вот некоторые из основных векторов инъекционных атак:

SQL-инъекция - злоумышленник вводит SQL-запрос в канал ввода конечного пользователя, такой как веб-форма или поле комментария. Уязвимое приложение отправит данные злоумышленника в базу данных и выполнит любые команды SQL, введенные в запрос. Большинство веб-приложений используют базы данных на основе языка структурированных запросов (SQL), что делает их уязвимыми для внедрения SQL. Новый вариант этой атаки - атаки NoSQL, нацеленные на базы данных, не использующие реляционную структуру данных.

Внедрение кода - злоумышленник может внедрить код в приложение, если оно уязвимо. Веб-сервер выполняет вредоносный код, как если бы он был частью приложения.

Внедрение команд ОС - злоумышленник может воспользоваться уязвимостью внедрения команд для ввода команд для выполнения операционной системой. Это позволяет атаке захватить данные ОС или захватить систему.

Внедрение LDAP - злоумышленник вводит символы для изменения запросов LDAP. Система уязвима, если в ней используются необработанные запросы LDAP. Эти атаки очень серьезны, потому что серверы LDAP могут хранить учетные записи пользователей и учетные данные для всей организации.

XML eXternal Entities (XXE) Injection - атака проводится с использованием специально сконструированных XML-документов. Это отличается от других векторов атак, поскольку использует уязвимости, присущие устаревшим синтаксическим анализаторам XML, а не непроверенные вводимые пользователем данные. XML-документы могут использоваться для обхода путей, удаленного выполнения кода и выполнения подделки запросов на стороне сервера (SSRF).

Межсайтовый скриптинг (XSS) - злоумышленник вводит текстовую строку, содержащую вредоносный код JavaScript. Браузер цели выполняет код, позволяя злоумышленнику перенаправить пользователей на вредоносный веб-сайт или украсть файлы cookie сеанса, чтобы захватить сеанс пользователя. Приложение уязвимо для XSS, если оно не дезинфицирует вводимые пользователем данные для удаления кода JavaScript [6].

Литература

1. Винокуров А.Ю. Традиционные криптографические алгоритмы. [Электронный ресурс] // Режим доступа: ww.enlight.ru/crypto/algorithms/algs. (дата обращения: 20.05.2021).
2. В МВД оценили ущерб от киберпреступлений в России в 2019 году [Электронный ресурс] // Официальный сайт телевизионной сети КГ - Режим

доступа: https://russian.rt.com/russia/news/696185-mvd-kiberprestuplenie-statistika (дата обращения: 01.07.2021).

3. Генпрокуратура заявила о низкой раскрываемости киберпреступлений [Электронный ресурс] // Официальный сайт газеты Известия - Режим доступа: https://iz.ru/987854/2020-03-17/genprokuror-krasnov (дата обращения: 20.06.2021).
4. Киберпреступность и киберконфликты: Россия [Электронный ресурс] // - Российский интернет-портал и аналитическое агентство Tadviser по теме корпоративной информатизации - Режим доступа: https://www.tadviser.ru/index.php/ (дата обращения: 10.06.2021).
5. Сидоренко Е. По цифровым следам: в РФ раскрывается лишь четверть киберпреступлений [Электронный ресурс] // Официальный сайт газеты Известия - Режим доступа: https://iz.ru/962966/ elena-sidorenko/po-tcifrovym-sledam-v-rf (дата обращения: 20.05.2021).
6. Центр политического анализа и информационной безопасности [Электронный ресурс] // Режим доступа: http://centerpolit.ru/content. php?id=59&now_month=9&now_year=2014 (дата обращения: 20.05.2021).

Literature

1. Vinokurov A.Yu. Traditional cryptographic algorithms. [Electronic resource] // Access mode: ww.enlight.ru/crypto/algorithms/algs. (date of access: 20.05.2021).
2. The Ministry of Internal Affairs assessed the damage from cybercrimes in Russia in 2019 [Electronic resource] // Official website of the KG television network - Access mode: https://russian.rt.com/russia/news/696185-mvd-kiberprestuplenie-statistika (date of access: 01.07.2021).
3. The Prosecutor General's Office announced the low detection rate of cybercrimes [Electronic resource] // Official website of the Izvestia newspaper - Access mode: https://iz.ru/987854/2020-03-17/genprokuror-krasnov (date of access: 20.06.2021).

4. Cybercrime and cyber conflicts: Russia [Electronic resource] // - Russian Internet portal and analytical agency Tadviser on the topic of corporate informatization - Access mode: https://www.tadviser.ru/index.php/ (date accessed: 10.06. 2021).
5. Sidorenko E. On digital traces: only a quarter of cybercrimes are disclosed in the Russian Federation [Electronic resource] // Official website of the Izvestia newspaper - Access mode: https://iz.ru/962966/ elena-sidorenko / po-tcifrovym-sledam-v -rf (date accessed: 20.05.2021).
6. Center for Political Analysis and Information Security [Electronic resource] // Access mode: http://centerpolit.ru/content. php? id = 59 & now_month = 9 & now_year = 2014 (date accessed: 20.05.2021).