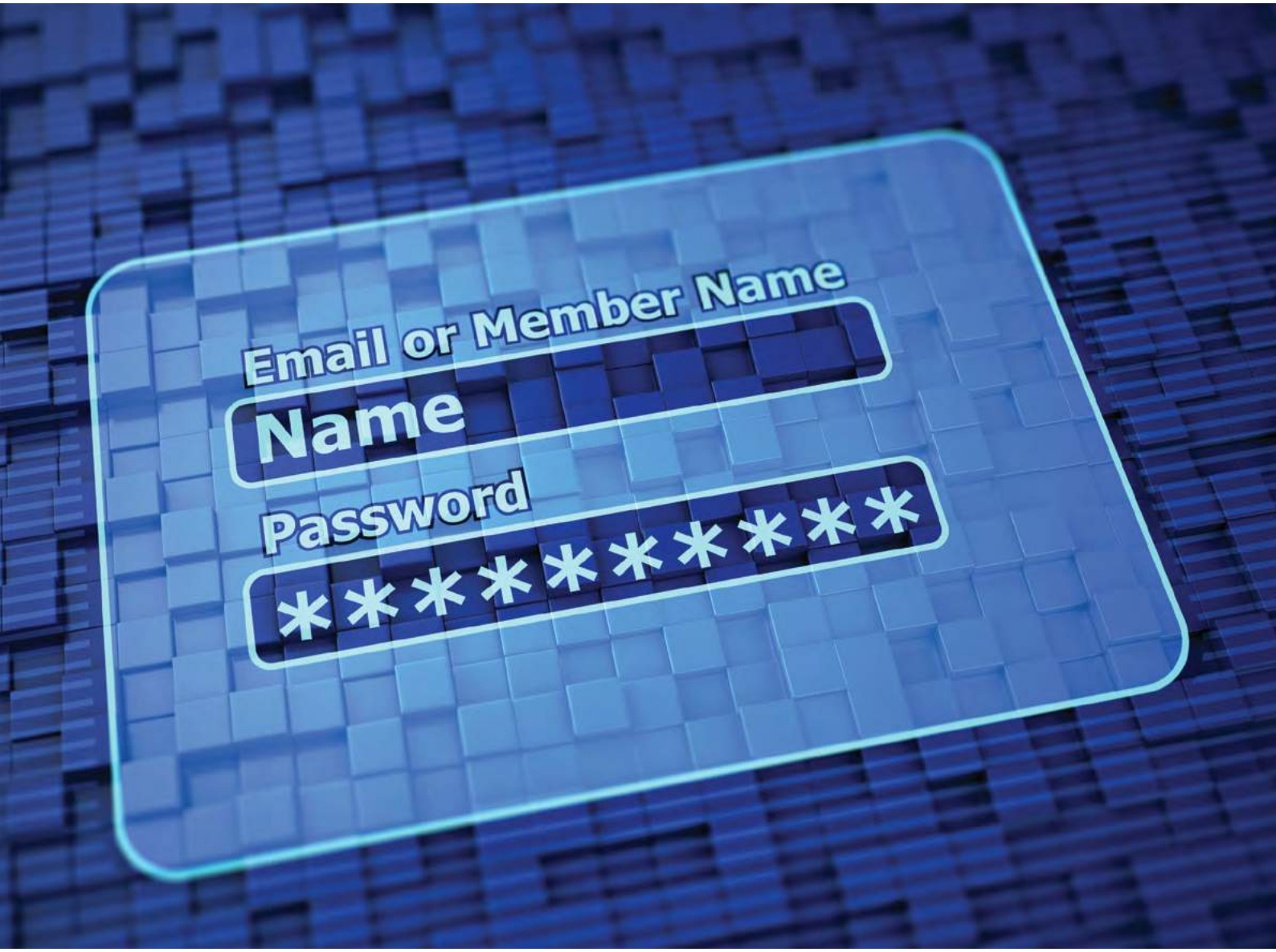

Аутентификация и управление доступом на предприятии

Парольная аутентификация подвергается серьезной и вполне обоснованной критике. Несостоятельность парольного доступа в контексте обеспечения корпоративной IT-безопасности сегодня очевидна.

Неудобные пароли

В современных компаниях для выполнения бизнес-задач сотрудники используют большое количество бизнес-приложений и информационных систем. При стандартном подходе к обеспечению безопасности это означает необходимость запоминать множество логинов и паролей, а также достаточно часто их менять согласно установленным политикам безопасности. Поэтому пользователи стараются использовать несложные пароли, дополнительно записывая их на бумажках, которые затем хранят в совершенно неподходящих для этого местах.

Кроме того, зачастую пользователи сами сообщают свои пароли коллегам в случае болезни или необходимости выполнения каких-то срочных действий. Поэтому даже если пользователь вводит пароль, это не означает, что он является владельцем предоставляемых учетных данных.

Неудобны пароли и для специалистов IT- и ИБ-служб. Забытые после отпусков пароли и заблокированные учетные записи требуют от них дополнительных затрат на восстановление этих данных.

«Неуправляемое» управление доступом

Другой проблемой, связанной с учетными данными, является управление доступом к данным и ресурсам компании. Прием новых и увольнение старых сотрудников, перестановки требуют от администраторов постоянной модификации данных о правах доступа, которые, в свою очередь, как показывает практика, часто неструктурированы, а потому управление ими затруднено и существует риск возникновения ошибок в таких изменениях. В результате в работе сотрудников, не получивших необходимый доступ, возникают вынужденные простои, а уволенные сотрудники могут по-прежнему получать доступ к корпоративным ресурсам и выполнять какие-то деструктивные действия.

Все это существенно снижает эффективность работы персонала. Но главное, что в такой ситуации возрастает риск несанкционированного доступа к ресурсам компании, а значит, существенно снижается общий уровень безопасности.

Для решения этих проблем используются технологии строгой аутентификации и единого доступа.

Строгая аутентификация

Одним из наиболее эффективных способов решения проблем использования парольного доступа является строгая (многофакторная) аутентификация, основанная на проверке дополнительных данных (факторов) для идентификации пользователя.

Факторами аутентфикации могут быть известная пользователю информация (пароль, PIN-код), имеющееся у пользователя устройство (смарт-карта, токен, генератор одноразовых паролей) или биометрические параметры пользователя (отпечаток пальца, рисунок вен на ладони, сетчатка глаза).

Аутентификация с применением каждого из этих факторов имеет свои преимущества и недостатки. Однако недостатки отдельных факторов легко устраняются путем применения комбинации нескольких параметров аутентификации. Очевидно, что чем больше факторов используется для аутентификации, тем она надежнее (наиболее распространенным является применение двух факторов).

Что касается выбора сочетания способов аутентификации к ресурсам целевой IT-инфраструктуры, это вопрос компромисса между удобством использования, полнотой интеграции, степенью безопасности и ценой итогового решения.

Кроме того, применение технологии строгой аутентификации обеспечивает автоматическое исполнение регламентов доступа к IT-системам компании.

Технология единого входа

Технология единого входа (Single Sign-On, SSO) обеспечивает возможность использовать один идентификатор для доступа ко всем (разрешенным) ресурсам и системам.

SSO-решения централизованно хранят все пароли пользователя и автоматически подставляют их в запросы аутентификации, когда это требуется.

То есть для того, чтобы выполнить вход в приложение, пользователю достаточно лишь предоставить данные для аутентификации (например, приложить палец к считывалю или выполнить какое-то иное действие в зависимости от используемой технологией аутентификации). Учетные данные (логин и пароль) будут подставлены SSO-системой автоматически без участия пользователя.

Таким образом, пользователи освобождаются не только от необходимости запоминания множества логинов и паролей, но также от необходимости их ручного ввода при аутентификации, что существенно упрощает доступ к приложениям и снижает нагрузку на IT- и ИБ-службы.

В концепции SSO также реализуется компонент управления правилами и политиками доступа ко множеству приложений и систем как для отдельных пользователей, так и для целых групп (отделов, подразделений и проч.), что делает прозрачным процесс управления учетными данными и паролями пользователей. При этом появляется важный «бонус» в виде возможности мгновенной блокировки доступа сразу во все системы в случае такой необходимости.

Комплекс решений Indeed ID

На отечественном рынке технологии строгой аутентификации и единого доступа успешно реализует комплекс решений Indeed ID, разработанный одноименной российской компанией и предназначенный для аутентификации и управления доступом на предприятии.

Данный комплекс поддерживает широкий спектр различных технологий строгой аутентификации (смарт-карты, токены и RFID-карты различных производителей, биометрия, одноразовые пароли), позволяя реализовать различные сценарии многофакторной аутентификации пользователей. Все поддерживаемые технологии можно комбинировать между собой. Например, можно аутентифицировать пользователей по отпечатку пальца и бесконтактной карте, смарт-карте и OTP и т.д. При этом, если на предприятии уже используются какие-то способы строгой аутентификации, они могут быть поддержаны данным комплексом благодаря особенностям архитектуры входящих в него решений, что особенно удобно, поскольку не требует дополнительных затрат на приобретение новых средств аутентификации и дает возможность гибко адаптировать систему аутентификации к потребностям и текущим условиям работы компании.

Подход Single Sign-On в масштабе предприятия реализует продукт Indeed Enterprise SSO, входящий в состав комплекса. Система централизованно хранит пароли пользователя от всех приложений, требующих аутентификации, и автоматически подставляет их, когда приложение этого требует. При истечении сроков действия паролей в приложениях система автоматически выполняет их смену.

Indeed Enterprise SSO подходит для любых типов приложений (Windows, Java, Web), независимо от их архитектуры: однозвенная, двухзвенная, трехзвенная, «толстый» клиент, «тонкий» клиент, терминальные приложения. При этом организовать доступ можно как в коробочные приложения, так и в приложения, разработанные на заказ.

Система также адаптирована к работе в терминальной среде (Remote Desktop, VDI, Citrix), что избавляет сотрудников от явного использования паролей в командировках и других ситуациях, когда работа с приложением выполняется в терминальной сессии.

В компаниях, использующих смарт-карты и токены, Indeed Enterprise SSO позволяет связать учетные данные пользователей с жизненным циклом ключевых носителей, интегрировав систему аутентификации с системами управления ключевыми носителями (Card Management System, CMS). Можно отметить, что в состав комплекса входит CMS-система этого же разработчика (Indeed Card Management), хотя при необходимости интеграция возможна и с другими системами данного класса, представленными на рынке.

В завершение следует отметить, что все действия администраторов и пользователей фиксируются в специальных журналах событий системы, что существенно упрощает процесс анализа и расследования инцидентов.