Эксперты бьют тревогу, предупреждая о серьёзных последствиях для критической инфраструктуры.

Известная киберпреступная группа Hunt3r Kill3rs заявила о взломе систем компании Schneider Electric, основанная в 1836 году, является международной компанией, которая производит и предоставляет решения для энергетических систем и автоматизации зданий. Она предлагает широкий спектр продуктов, включая системы электропитания, автоматические выключатели, контроллеры, преобразователи частоты и другое оборудование." data-html="true" data-original-title="Schneider Electric" >Schneider Electric в Германии и краже конфиденциальных данных. Сообщение об этом появилось на странице платформы ThreatMon, известной отслеживанием разнообразных киберугроз и их активности.

В своём посте хакеры Hunt3r Kill3rs утверждают, что проникли в системы Schneider Electric и получили доступ к конфигурациям счётчиков PowerLogic ION7650, которые являются важной частью систем управления энергопотреблением.

Schneider Electric, мировой лидер в области управления энергией и автоматизации, имеет значительное присутствие в Германии. Это делает взлом особенно тревожным для компании и её клиентов в пределах страны.

Точная природа инцидента пока не раскрыта, но эксперты предполагают, что последствия могут быть серьёзными, учитывая роль Schneider Electric в управлении критической инфраструктурой. Компания пока не выпустила официального заявления, однако, по данным источников, внутреннее расследование уже идёт.

Эксперты по кибербезопасности выражают обеспокоенность по поводу взлома, отмечая растущую сложность действий киберпреступных групп, таких как Hunt3r Kill3rs.

«Этот инцидент подчёркивает острую необходимость в надёжных мерах кибербезопасности, особенно для компаний, занимающихся критической инфраструктурой», — заявила доктор Лаура Штайн, аналитик по кибербезопасности из Берлинского технологического института.

«Последствия таких взломов могут быть катастрофическими, влияя не только на компанию, но и на экономику и общественную безопасность в целом».

В ответ на взлом немецкие власти начали всестороннюю проверку протоколов

Все права защищены

save pdf date >>> 28.01.2026

кибербезопасности для компаний, связанных с критической инфраструктурой.

Федеральное управление по информационной безопасности было проинформировано о случившемся и сотрудничает со Schneider Electric для оценки масштаба взлома и минимизации возможного ущерба.

Этот инцидент служит напоминанием о постоянной угрозе со стороны киберпреступников и необходимости непрерывной бдительности и инвестиций в кибербезопасность.

По мере продолжения расследования ожидается, что как Schneider Electric, так и немецкие власти предоставят дополнительную информацию о случившемся.

На перекрестке науки и фантазии — наш канал

Все права защищены

save pdf date >>> 28.01.2026