Smart Reading

САММАРИ
& ЛУЧШИЕ ИДЕИ ИЗ КНИГ

КИБЕРБЕЗОПАСНОСТЬ ДЛЯ БИЗНЕСА

Ларри Клинтон

Cybersecurity for Business. Organization-Wide Strategies to Ensure Cyber Risk is Not Just an IT Issue
Larry Clinton

Smart Reading

Кибербезопасность для бизнеса. Как сделать защиту от киберугроз задачей всей компании. Ларри Клинтон. Саммари

Серия «Smart Reading. Ценные идеи из лучших книг. Саммари»
Серия «Впервые на русском (Smart Reading)»

http://www.litres.ru/pages/biblio_book/?art=73903977
Кибербезопасность для бизнеса. Как сделать защиту от киберугроз задачей всей компании. Ларри Клинтон. Саммари:

Аннотация

Это саммари – сокращенная версия книги «Кибербезопасность для бизнеса. Как сделать защиту от киберугроз задачей всей компании» Ларри Клинтона. Только самые ценные мысли, идеи, кейсы, примеры.

«Кибербезопасность для бизнеса» – это подробное руководство по современным принципам защиты бизнеса от киберугроз. Автор предлагает взглянуть на киберзащиту как на комплексную управленческую задачу и выступает своего рода переводчиком с технического языка на экономический. Как оценить киберугрозы в деньгах? Как настроить процессы, чтобы киберзащита работала? Какие моменты в деятельности компании делают ее особенно уязвимой для хакеров? Какова роль различных подразделений в общей информационной безопасности и как создать в компании культуру кибербезопасности? Автор, возглавляющий глобальную некоммерческую организацию по интернет-безопасности, делится своим опытом и советами, основанными на многолетней реальной практике.

Содержание

Принципы кибербезопасности для современной компании 6
Кибербезопасность – элемент стратегии бизнеса 8
Наперегонки с хакерами 10
Конец ознакомительного фрагмента. 12

Smart Reading Кибербезопасность для бизнеса. Как сделать защиту от киберугроз задачей всей компании. Ларри Клинтон. Саммари

Оригинальное название:
Cybersecurity for Business. Organization-Wide Strategies to Ensure Cyber Risk is Not Just an IT Issue

Автор:
Larry Clinton

Принципы кибербезопасности для современной компании

Каждый бизнесмен хочет, чтобы его компания развивалась и добивалась успеха, и, конечно, каждый желает защитить свое дело от всех возможных угроз. Экономисты, юристы и аудиторы ежедневно вносят понятный каждому руководителю вклад в безопасность бизнеса. Но когда дело касается киберсреды, часто возникает растерянность. Как оценить киберриски с точки зрения финансов? Какие организационные приемы нужны, чтобы сделать киберзащиту компании максимально эффективной? Как ставить задачи перед разными подразделениями и какой вклад вносит каждый сотрудник в создание общего киберщита для компании?

Книга «Кибербезопасность для бизнеса» отвечает на вопросы о кибербезопасности с точки зрения корпоративного управления. Собственники и управляющие компаниями с ее помощью смогут разобраться в источниках угроз и моделях защиты и управлять киберзащитой так же, как решением других важных для бизнеса задач. Автор, который возглавляет Альянс интернет-безопасности (ISA), действующий на четырех континентах Земли, подчеркивает, что ***кибербезопасность – это не только техническая проблема, но и стратегический вопрос, требующий комплексного***

подхода если не на государственном уровне, то как минимум на уровне всей компании.

А чтобы освоить такой подход, интересно и полезно узнать об эволюции кибератак, постоянном расширении рамок базовых мер кибергигиены и о том, как правильно интегрировать меры по кибербезопасности в стратегию управления компанией.

Кибербезопасность – элемент стратегии бизнеса

Компании часто ошибочно рассматривают кибербезопасность как исключительно техническую задачу, что приводит к недостаточному финансированию и неэффективным стратегиям. Киберпреступность наносит огромный ущерб мировой экономике, и за пугающими цифрами стоят конкретные истории взломов, утечек и потерь, которые причиняют реальный урон компаниям по всей планете.

> *По оценкам Всемирного экономического форума, ущерб от киберпреступности в 2020 году составил $2 трлн и продолжает расти опережающими темпами.*

Цифровая трансформация – требование для каждого современного бизнеса, который хочет достойно конкурировать в своей отрасли. Но ***технический прогресс, открывающий новые коммерческие возможности, также увеличивает уязвимость к кибератакам.*** Среди сравнительно новых факторов риска автор называет:

- распространение мобильных и облачных технологий, которое серьезно повышает риски утечки корпоративных и

личных данных и требует внедрения новых мер кибербезопасности;

- развитие инструментов искусственного интеллекта (ИИ), которые злоумышленники используют для создания все более изощренных атак. Атаки с использованием ИИ особенно опасны из-за высокой способности алгоритмов анализировать и обходить установленные защиты;
- переход большого числа сотрудников на удаленку: пандемия COVID-19 резко ускорила этот процесс и вызвала взрывной рост числа кибератак. Риски утечки данных еще выше там, где для работы используются личные устройства;
- перенос операций, хранения данных и средств обеспечения безопасности в облачную инфраструктуру.

Если компания хочет устойчиво расти, ее кибербезопасность должна развиваться вместе с процессами основного бизнеса.

Наперегонки с хакерами

Начиная с 1990-х годов и по настоящее время Американский национальный институт стандартов NIST (National Institute of Standards and Technology) публикует стандарты компьютерной безопасности с детальными разъяснениями и рекомендациями. Однако, к сожалению, предлагаемые меры недостаточны, потому что не способны опередить эволюцию угроз, возникающих в цифровой среде.

Киберугрозы эволюционируют быстро. Злоумышленники придумывают все новые способы нападения, включая персонализированные атаки и продвинутое программное обеспечение, для осуществления своих преступных целей.

Самые передовые и вредоносные на сегодня – атаки типа Advanced Persistent Threats (APT, продвинутая постоянная угроза). В таких атаках используются сложные, нестандартные методы, часто с применением нулевых уязвимостей (тех, о которых еще не догадывается жертва кибератаки) и социальной инженерии (то есть с использованием человеческих слабостей для взлома защиты). APT-атаки дают злоумышленникам возможность проникать внутрь системы и долгое время оставаться незамеченными, а их цели – кража данных, шпионаж или даже разрушение инфраструктуры.

APT-атаки обычно нацелены на крупные компании или даже правительственные организации, которые имеют дело со сверхсекретными данными, например с военными и финансовыми вопросами или патентами.

Этапы APT-атаки:

1) проникновение в сеть, например с помощью фишингового электронного письма или вредоносного вложения;

2) поиск уязвимостей: вредоносное программное обеспечение исследует уязвимости и обменивается данными с внешними серверами;

3) установка дополнительных точек взлома – это нужно, чтобы гарантировать продолжение атаки, если определенная точка входа или уязвимость будет раскрыта и защищена;

4) вредоносная деятельность в сети, к примеру сбор учетных записей и паролей, хищение конфиденциальных файлов или удаление важных данных.

Чтобы действовать на опережение и надежно защищать свои данные и системы, бизнес уже не может рассчитывать только на соответствие нормативным требованиям. ***Динамика развития киберугроз требует выхода за рамки стандартных шаблонов***

Конец ознакомительного фрагмента.