КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КАЛИНИНГРАД

08.06.2023

Йоханн Воронин

- Дипл.Инж. Бизнес-Информатика, университет Дортмунд
- PMP®, Project Management Institute
- Scrum Master® & Product Owner®
- Специалист по информационной безопасности и политики конфиденциальности персональных данных

ТОМ

ТОМ или ТОМ — это меры, которые предназначены для обеспечения безопасности обработки персональных данных при защите данных.

Примеры технических мер

- Технически установленные требования к сложности пароля
- Заборы и другая конструктивная защита помещений или зданий оконные и дверные замки системы сигнализации
- Псевдонимизация шифрования персональных данных учетные записи пользователей
- Требования к паролю или другие процессы идентификации пользователя, например, посредством процесса биометрического сканирования.
- автоматическое создание журналов (т.н. логирование)

Примеры организационных мер

- Например, существует так называемый принцип четырех глаз для определенных процессов, задач или решений. В некоторых областях это могут делать не менее двух ответственных лиц.
- Политика входа посетителей
- Руководство по использованию ИТ, Интернета или мобильных устройств
- Инструкция по утилизации документов с персональными данными в соответствии с требованиями защиты данных
- Декларация о приверженности конфиденциальности данных

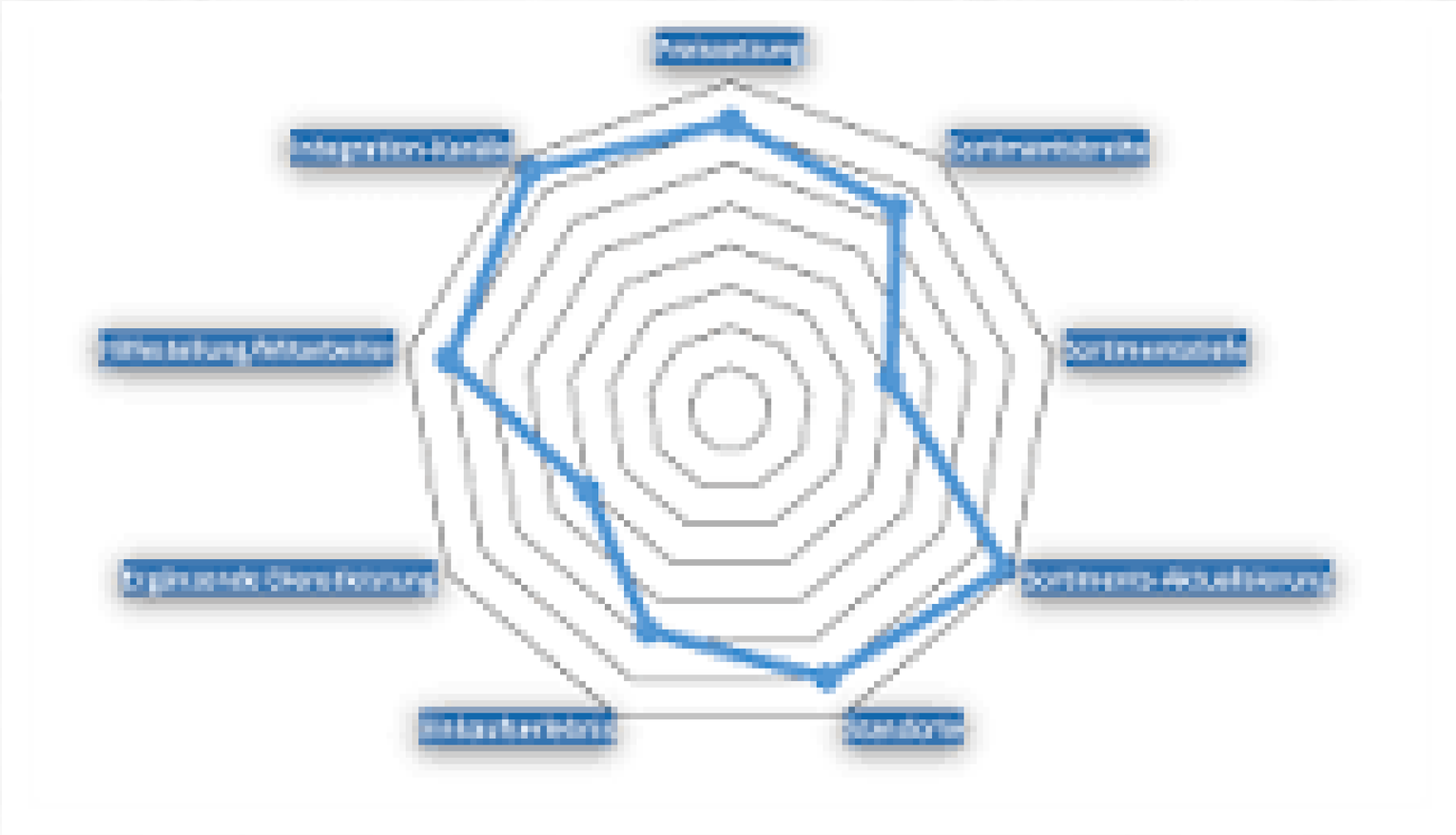
Технические и организационные мероприятия в компании

ТОМ обычно влияет на всю компанию, но также и на отдельные отделы. Это связано с тем, что некоторые ТОМ должны быть адаптированы к индивидуальным обстоятельствам отделов, чтобы обеспечить наилучшую возможную защиту персональных данных. Поэтому компаниям рекомендуется включать свои технические и организационные меры в аудит защиты данных и одновременно проводить оценку текущего уровня безопасности.

Технические и организационные мероприятия в компании

ТОМ обычно влияет на всю компанию, но также и на отдельные отделы. Это связано с тем, что некоторые ТОМ должны быть адаптированы к индивидуальным обстоятельствам отделов, чтобы обеспечить наилучшую возможную защиту персональных данных. Поэтому компаниям рекомендуется включать свои технические и организационные меры в аудит защиты данных и одновременно проводить оценку текущего уровня безопасности.

Аудит



1. Контроль доступа к помещениям

Контроль доступа — одна из классических мер в технической и организационной сфере для соблюдения защиты данных. Под контролем доступа понимаются все меры, запрещающие посторонним лицам доступ в помещения, здания или помещения, в которых расположены системы обработки данных и обрабатывающие персональные данные.

2. Контроль доступа к техники

В отличие от контроля доступа, контроль доступа направлен на предотвращение несанкционированного использования систем обработки данных. Системы обработки данных, такие как компьютерные системы, должны использоваться только лицами, имеющими соответствующие полномочия на их использование.

3. Контроль доступа к системам

В этом контексте пользователи могут использовать системы обработки данных только в той степени, в которой это разрешено настроенной авторизацией доступа. Этот контроль доступа гарантирует, что никто не сможет обрабатывать личные данные без их разрешения.

4. Управление передачей

Под контролем передачи понимаются меры, обеспечивающие безопасность персональных данных при передаче данных. Передача данных в этом смысле означает электронную передачу, транспортировку и хранение персональных данных. Обеспечение безопасности персональных данных во время этой передачи является целью контроля передачи и, следовательно, имеет важное значение для защиты данных.

5. Контроль ввода

Контроль ввода ТОМ связан с проверяемостью обработки данных. Меры в этом сегменте предназначены для обеспечения контроля ввода данных, изменения данных и удаления данных.
Установив меры в этой области, можно точно проверить, кто ввел, изменил или удалил какие персональные данные в системах обработки данных.

6. Контроль заказа

Контроль заказа актуален всегда, когда происходит обработка заказа. Затем необходимо убедиться, что обработка осуществляется в соответствии с инструкциями клиента.

7. Контроль доступности и возможность восстановления

Благодаря контролю доступности и возможности восстановления ТОМ личные данные должны быть защищены от уничтожения или потери, чтобы их можно было восстановить в случае сбоя.

8. Контроль разделения

Если персональные данные были собраны для разных целей, необходимо обеспечить, чтобы они также обрабатывались отдельно, так называемый контроль разделения.

9. Управление носителями иформации

Контроль носителей данных заключается в предотвращении несанкционированного чтения, копирования, изменения или стирания носителей данных

10. Контроль памяти

В отличие от входного контроля речь идет не о проверяемости обработки данных, а о предотвращении несанкционированной обработки данных.

11. Пользовательский контроль

Пользовательский контроль предназначен для предотвращения использования автоматизированных систем обработки данных посторонними лицами с помощью передачи данных.

12. Целостность данных

Целостность данных ТОМ включает в себя обеспечение того, что сохраненные личные данные не могут быть повреждены из-за сбоев в работе системы. Это включает, например, создание и настройку концепции резервного копирования и восстановления.

Целесообразность

Необходимо учитывать экономическую адекватность.

Например, ТОМ малого бизнеса не может иметь такие же стандарты во всех областях, как ТОМ крупной корпорации по экономическим причинам.

Готов ответить на ваши вопросы

E-mail: jvoronin@gmail.com
Phone: +7 906 219 66 00