



Стратегия за киберсигурност

Съдържание:

1. Въведение, контекст и регулаторни изисквания	3
2. Изисквания и очаквания към компаниите в обхвата на NIS2	3
2.1 Управление на риска	3
2.2 Докладване на инциденти	3
2.3 Сигурност на веригата за доставки	3
2.4 Надзор и прилагане	4
3. Стратегически цели	4
4. Конкретни мерки за подобряване на киберсигурността	5
4.1 Приложими регулаторни изисквания за киберсигурност	5
4.2 Система за управление на информационните активи	5
4.3 Мониторинг и управление на информационната сигурност	6
5. Стойност и изисквания за идентифицираните мерки за подобрене	6
5.1 Разработване на документация	6
5.2 Система за управление на информационните активи	8
5.3 Услуга за мониторинг и управление на информационната сигурност	8
5.4 Допълнителна информация относно очакваните стойности	10

1. Въведение, контекст и регулаторни изисквания

Република България и Европейският съюз признаха защитата на информацията и киберсигурността за ключови приоритети поради експоненциално нарастващите заплахи във всички сектори на обществения и социалния живот.

С въвеждането на *Директива (ЕС) 2022/2555 относно мерки за високо общо ниво на киберсигурност в Съюза (NIS2)*, дружество „Бони Холдинг“ е изправено пред допълнителни задължения в областта на киберсигурността, по-специално поради наличието на изследователски институт с шест центъра за изследвания и консултации.

Понастоящем специфичният регламент, отнасящ се до киберсигурността, е *Наредбата за минималните изисквания за мрежова и информационна сигурност*, приета с ПМС № 186 от 26.07.2019 г. (обнародвана в ДВ, бр. 59 от 26.07.2019 г.). Очаква се актуализираната ѝ версия да се прилага за субекти, попадащи в обхвата на *Директива (ЕС) 2022/2555*.

2. Изисквания и очаквания към компаниите в обхвата на NIS2

За да се съобрази с NIS2, дружество „Бони Холдинг“ трябва да е готов да демонстрира следното по време на одити от регулаторни органи или втори страни:

2.1 Управление на риска

- Редовни оценки на риска, включително мерки за смекчаване на идентифицираните рискове. Тези оценки разглеждат специфични заплахи за активите и дейностите на организацията, както и известни уязвимости. Трябва да се разработи план за разработване с конкретни действия и срокове.
- Периодични тестове за проникване и одити за сигурност.

2.2 Докладване на инциденти

- Организацията трябва да докладва за значителни инциденти в рамките на 24 часа от възникването им. Изключително важно е да се демонстрира способност за откриване на инциденти и събиране на цифрови доказателства и артефакти.
- В рамките на един месец трябва да бъде представен окончателен доклад, в който подробно се описва инцидентът, засегнатите трети страни и системи, както и предприетите мерки за предотвратяване на повторение.

2.3 Сигурност на веригата за доставки

- Трябва да се въведат мерки за управление на рисковете от доставчици и трети страни, като се акцентира върху устойчивостта на веригата за доставки.

- Оценка на информационната сигурност на доставчиците и/или включване на специфични договорни изисквания.

2.4 Надзор и прилагане

- Директивата налага по-строг надзор от страна на националните органи, включително редовни одити и проверки на място, както е посочено в предложението на нов *Закон за киберсигурността*.
- Компетентните органи ще имат правомощието да изискват информация и да имат достъп до документи, за да гарантират спазването на изискванията.

3. Стратегически цели

Стратегическите цели на „Бони Холдинг“ в областта на киберсигурността са насочени към осигуряване на устойчивост и предвидимост на ИТ-зависимите производствени процеси и бизнес дейности. Това включва внедряването на нови технологии, инструменти за киберсигурност, услуги и документация, съобразени с анализа на риска.

Ключовите цели включват:

- Внедряване на ефективен процес за управление на киберсигурността в съответствие с *Наредбата за минималните изисквания за мрежова и информационна сигурност*.
- Осигуряване на киберустойчивост чрез внимателно подбрани инструменти и технологии.
- Намаляване на риска от киберинциденти чрез непрекъснато наблюдение и поведенчески анализ на системите и потребителите.
- Постигане на готовност за откриване, докладване и реагиране на инциденти, за да се сведат до минимум потенциалните щети.
- Управление на известни и нововъзникващи уязвимости чрез подобряване или въвеждане на нови контрамерки.
- Определяне на ролята и отговорностите за управление на ИТ и киберсигурността в дружеството.
- Провеждане на информирани оценки на риска, последвани от осъществими планове за разработка.
- Ефективно използване на публични средства за подкрепа на киберсигурността и ИТ операциите.

- Възлагане на външни доставчици на дейности, които не могат да бъдат поддържани вътрешно поради липсата на персонал.
- Документиране и актуализиране на отговорностите, дейностите и процесите, свързани с ИТ и киберсигурността.
- Осигуряване на постигането на бизнес целите чрез ефективни мерки за сигурност, поддържащи ИТ-зависими операции.
- Въвеждане на процес за управление на услугите, предоставяни на обучаващи се, като устойчивостта и сигурността са ключови показатели за успех.

4. Конкретни мерки за подобряване на киберсигурността

Във връзка с предходния раздел беше извършен анализ на текущото състояние на ИТ инфраструктурата в „Бони Холдинг“. Заключениета от този доклад доведоха до създаването на списък с краткосрочни (неотложни) цели за подобряване на киберсигурността. Този списък не е изчерпателен по отношение на необходимите реформи или технологични подобрения, но служи като солидна отправна точка за бъдещото развитие на киберсигурността в дружеството.

4.1 Приложими регулаторни изисквания за киберсигурността

Очаква се актуализация на действащата *Наредба за минималните изисквания за мрежова и информационна сигурност*. Тя ще въведе задължителни мерки за подобряване на киберсигурността, а „Бони Холдинг“ попада в нейния обхват и изисквания за одит.

От съществено значение е да се даде приоритет на спазването на тази наредба, тъй като неспазването на изискваните мерки и неподдържането на отчетност може не само да навреди на репутацията на компанията, но и да доведе до административни санкции от регулаторните органи.

За тази цел трябва да се разработи подробна документация, която да отразява действителното състояние на процесите, свързани със сигурността в „Бони Холдинг“ в контекста на Наредбата. По отношение на *Директива (ЕС) 2022/2555*, Българското законодателство все още е в процес на хармонизиране и се очаква новите мерки да допълнят и разширят съществуващата *Наредба за минималните изисквания за мрежова и информационна сигурност*

4.2 Система за управление на информационните активи

Внедряването на система за управление на информационната сигурност изисква непрекъсната поддръжка и пълен поглед върху активите, които тя е предназначена да защитава. Универсално приложима мярка в тази област е въвеждането на система за управление на ИТ активите (ITAM).

„Бони Холдинг“ трябва да планира внедряването на такава система като единствен начин за контрол на броя, състоянието и текущото състояние на ИТ активите в рамките на своята инфраструктура. Тъй като оценките на риска, задължителни по закон, се фокусират конкретно върху организационните активи, внедряването на тази технология се счита за изключително важно.

4.3 Мониторинг и управление на информационната сигурност

Надеждността и ефективността на системата за управление на информационната сигурност се доказват от способността ѝ да наблюдава и реагира на заплахи в реално време. Не е достатъчно да се разчита единствено на технически контроли, без да се включат потребителски действия, DNS заявки, уязвимости и метаданни, генерирани от различни системи в „Бони Холдинг“.

Следователно, стратегията за подобрене включва внедряването на SIEM (Система за управление на информацията и събитията в сигурността), която ще осигури пълен поглед върху инфраструктурата и ще позволи управление на уязвимостите. Осъзнавайки сложността на внедряването на такава платформа, „Бони Холдинг“ разглежда възлагането ѝ на трета страна външен доставчик като жизнеспособна опция. Този подход осигурява достъп до необходимата експертиза, внедряване, поддръжка и разследване на инциденти – вече широко възприета практика сред публичните организации. Проучванията в тази област също показват значителни икономии на разходи с този модел.

5. Стойност и изисквания за идентифицираните мерки за подобрене

5.1 Разработване на документация

Този процес вече е започнал, с определен изпълнител и определени срокове. Финализирането на документацията зависи от спецификата на предстоящия *Закон за киберсигурността*, който ще транспонира изискванията на NIS2 в българското законодателство.

Междувременно е създадена първата версия на Политиката за информационна сигурност. Тя ще бъде допълнена със следното съдържание/документи:

1.	Политика за мрежова и информационна сигурност
2.	Класификация на информацията
3.	Формуляр за класификация на информацията
4.	Управление на риска
5.	Оценка на риска
6.	Управление на информационните активи
7.	Инвентаризация на информационните активи
8.	Сигурност на човешките ресурси

9.	Декларация за поверителност
10.	Споразумение за поверителност с трети страни
11.	Управление на взаимодействията с трети страни
12.	Управление на промените за информационните активи
13.	Промяна на плана
14.	Сигурност при разработването и придобиването на информационни и комуникационни системи
15.	Филтриране на трафика
16.	Списък на забранените портове за входящ/изходящ трафик
17.	Неразрешено използване на устройства
18.	Криптография
19.	Администрация на информационните и комуникационните системи
20.	Списък с администраторски акаунти
21.	Доклад за състоянието на мрежовата и информационната сигурност
22.	План за мониторинг и контрол
23.	Административна среда
24.	Диаграма на свързаността
25.	Управление на достъпа
26.	Формуляр за заявка/промяна/прекратяване на достъп
27.	Матрица за достъп до информационни и комуникационни системи (ИКС)
28.	Защита от отдалечен достъп/дистанционна работа
29.	Защита на хардуерните устройства
30.	Защита на софтуера и фърмуера
31.	Списък с одобрен софтуер
32.	Защита от злонамерен софтуер
33.	Защита на уеб сървъра
34.	Защита на системата за имена на домейни (DNS)
35.	Физическа сигурност
36.	Мониторинг
37.	Контролен списък
38.	Системни лог-файлове /дневници/
39.	Управление на инциденти, свързани с мрежовата и информационната сигурност
40.	Регистър на инциденти
41.	Класификация и приоритет на инцидентите
42.	Известие за инцидент
43.	Резервно копие /бекъп/ и архивиране на данни

44.	График за изготвяне на резервно копие /бекъп/ и архивиране на данните
45.	Резервно копие /бекъп/ на инфраструктурни компоненти
46.	Планове за осигуряване на непрекъснатост на бизнеса
47.	Програма за тестване на плана

5.2 Система за управление на информационните активи

Внедряването на система за управление на информационните активи е от основно значение за ефективното управление на киберсигурността. Според специализиран контролен списък, публикуван от Центъра за интернет сигурност, наличието на система за управление на активите е първият елемент в техните въпросници за оценка. Този подход е възприет и от българските регулаторни органи със същата цел – да идентифицират и управляват всички устройства, свързани към инфраструктурата на организацията.

Предложихме тестван продукт – runzero – който е бърз и лесен за внедряване и предоставя много подробна статистика за това какво е свързано с инфраструктурата на „Бони Холдинг“ във всеки един момент. Продуктът е достъпен за директно закупуване от уебсайта на производителя.

5.3 Услуга за мониторинг и управление на информационната сигурност

Тази услуга следва да включва необходимите лицензи за облачна платформа за SIEM (Система за управление на информацията и събитията в сигурността) и система за управление на уязвимостите. Тя следва да обхваща цялата инфраструктура на „Бони Холдинг“ и да включва разходи за набор от дейности и технологии, които напълно отговарят на настоящите регулаторни изисквания.

Чрез внедряването на подобно решение, „Бони Холдинг“ ще може да:

- Демонстрира способността си за откриване на инциденти,
- Събиране на доказателства,
- Защита на метаданните (лог-файловете/дневниците) от манипулация и изтриване,
- И проследяване на действията на администратора и потребителя в контекста на киберсигурността.

Характеристики на услугата	
1.	Мониторинг и реагиране на сигнали за зловреден софтуер въз основа на приоритети, определени в документацията.
2.	Мониторинг на актуализации на модули, сигнатури и продуктови версии, както и идентифициране на компютри/активи, които не са свързани към конзолата за управление в ИТ средата на „Бони Холдинг“.

3.	Управление на групи за защита на потребителите и техните конфигурации.
4.	Управление на политики за сигурност, свързани със защита от зловреден софтуер, съобразени с текущите нужди.
5.	Интеграция и поддръжка с MS Active Directory Services.
6.	Процеси на мониторинг, инициирани по време на изпълнението на дадена програма.
7.	Мониторинг на състоянието на наскоро свързаните критични активи.
8.	Конфигуриране и проверка на сканирания при поискване на крайни точки и сървъри.
9.	Редовни месечни проверки на публичните уеб-базирани приложения на „Бони Холдинг“, както и при поискване от страна на Клиента.
10.	Съдействие и насоки на разработчиците на уеб платформи на „Бони Холдинг“ за отстраняване на идентифицирани уязвимости.
11.	Повторна проверка и верификация след отстраняване на уязвимостите.
12.	Актуализиране и конфигуриране на скенери и тяхното разполагане в инфраструктурата на „Бони Холдинг“.
13.	Извършване на удостоверени сканирания с помощта на Selenium скриптове за по-задълбочен анализ на приложенията.
14.	Анализ на ефективността на предприетите действия за отстраняване на уязвимостите.
15.	Конфигуриране и поддръжка на сканиращи агенти и агенти за инвентаризация.
16.	Агрегиране на метаданни и лог-файлове /дневници/ от критични ИТ системи или други системи, посочени от Клиента.
17.	Разработване на различни сценарии за автоматизация за подобряване на мерките за сигурност.
18.	Ежедневно наблюдение и анализ на метаданни от избраната платформа.
19.	Съпоставяне и обработка на събраните данни за извличане на информация за заплахи, инциденти или злонамерени опити, насочени към инфраструктурата на „Бони Холдинг“.
20.	Ръчен преглед на докладваните инциденти за определяне на техния статус (фалшиво положителни, наистина положителни) преди препращането им за по-нататъшна обработка от екипа на „Бони Холдинг“ или трета страна.
21.	Подготовка и скриптиране на лог парсери за нестандартни системи в инфраструктурата на Бони Холдинг.
22.	Подобряване или интегриране с нови услуги на „Бони Холдинг“ по време на договорния период.
23.	Доставчикът на услуги трябва да може да предостави информация от регистрационните файлове на SIEM (Системата за управление на информацията и събитията в сигурността) в случай на разследване на инциденти или анализ на аномалии.

24.	Поддръжка, оказвана за екипа на „Бони Холдинг“ с реални данни за съставяне и актуализиране на регистъра на риска.
25.	Консултиране на екипа на „Бони Холдинг“ относно актуализиране на съществуващи политики/процедури или вътрешни правила, свързани с информационната сигурност.
26.	Консултации относно актуализиране на диаграми, схеми, конфигурационни листове, архитектура или други елементи в зависимост от бизнес модела на организацията и използваните технологии.
27.	Редовни срещи с екипа на „Бони Холдинг“ за анализ и планиране на действия за намаляване на рисковете от текущи заплахи за ИТ
28.	Анализ на уязвимостите на инфраструктурата на „Бони Холдинг“, придружен от препоръки за отстраняване от отговорния екип или външния доставчик.
29.	Потвърждение за отстраняване на уязвимостта след проверка до успешно разрешаване.

5.4 Допълнителна информация относно очакваните стойности

Планираната платформа за внедряване на услугата, описана в раздел 5, е Rapid7 InsightIDR/InsightVM, обхващаща приблизително 400 актива. Тези активи включват комбинация от компютри на служителите (както настолни, така и мобилни), сървъри и мрежови устройства.

Камерите, DVR, принтерите и специализираните машини предават данните си по различен начин към платформата на SIEM (Система за управление на информацията и събитията в сигурността) и не подлежат на лицензиране.

