30 точки за проверка на готовността за ОТ сигурност

За оператори на индустриални обекти. Приоритети, практически насоки за всяка точка и реалистичен ред за първите 18 месеца.

30-ТЕ ТОЧКИ ПО ОБЛАСТИ		● Поправете първо	● Поправете тази година	● Изграждайте с времето		
1	Знайте какво управлявате	3	1 2 4 5			
2	Отдалечен достъп	6 7 8	9 10			
3	Разделяне на мрежите	11 12	14 15	13		
4	Акаунти, пароли и устройства	16 20	17 19	18		
5	Резервни копия и възстановяване	21 22 23	24	25		
6	Готовност за инциденти	26	27 29	28 30		

ПРЕДИ ДА ЗАПОЧНЕТЕ

Как да използвате списъка

1

Кой

Ръководителят на експлоатацията или човекът, който най-добре познава системите за управление, заедно с този, който се грижи за ИТ на обекта. Отделете един час.

2

Как

Прочетете всяка точка и отговорете с „Да“, „Отчасти“ или „Не“. „Мислим, че да“ е „Отчасти“. Запишете доказателството за всяко „Да“: документ, екран, лог. „Да“ без доказателство е „Отчасти“.

3

След това

Пребройте отговорите „Да“. Поправете първо пропуските с Приоритет 1, после с Приоритет 2, после с Приоритет 3. Планът към края показва реалистичен ред.

Трите приоритета

ПРИОРИТЕТ 1 — **11** точки

Поправете първо

СЛЕДВАЩИТЕ 30 ДО 90 ДНИ

Пряк вход за нападател или това, което решава дали ще си върнете обекта след инцидент.

3 6 7 8 11 12 16 20 21 22 23

ПРИОРИТЕТ 2 — **14** точки

Поправете тази година

3 ДО 9 МЕСЕЦА

Основите, благодарение на които Приоритет 1 се задържа и за които одиторът ще попита.

1 2 4 5 9 10 14 15 17 19 24 26 27 29

ПРИОРИТЕТ 3 — **5** точки

Изграждайте с времето

9 ДО 18 МЕСЕЦА

Стъпки към зрялост. Важни са, но едва след като Приоритет 1 и 2 са налице.

13 18 25 28 30

За оценките на труда. Трудът е груб ориентир за един средно голям обект с 50 до 300 устройства за управление. Това е време на вашите служители, а не календарно време, и не включва покупката на оборудване.

Какво има в документа

01	**Карта за оценка**	една страница за разпечатване и попълване
02	**Къде се прилагат точките**	мрежовите зони на една схема
03	**30-те точки**	как изглежда доброто, как се прави, кой, труд
04	**Реалистичен ред**	от първите 30 дни до 18-ия месец
05	**Вашият резултат**	какво означава резултатът ви и какво следва

РАЗПЕЧАТАЙТЕ ТАЗИ СТРАНИЦА

Карта за оценка

Отбележете едно квадратче за всяка точка. Цветът показва приоритета.

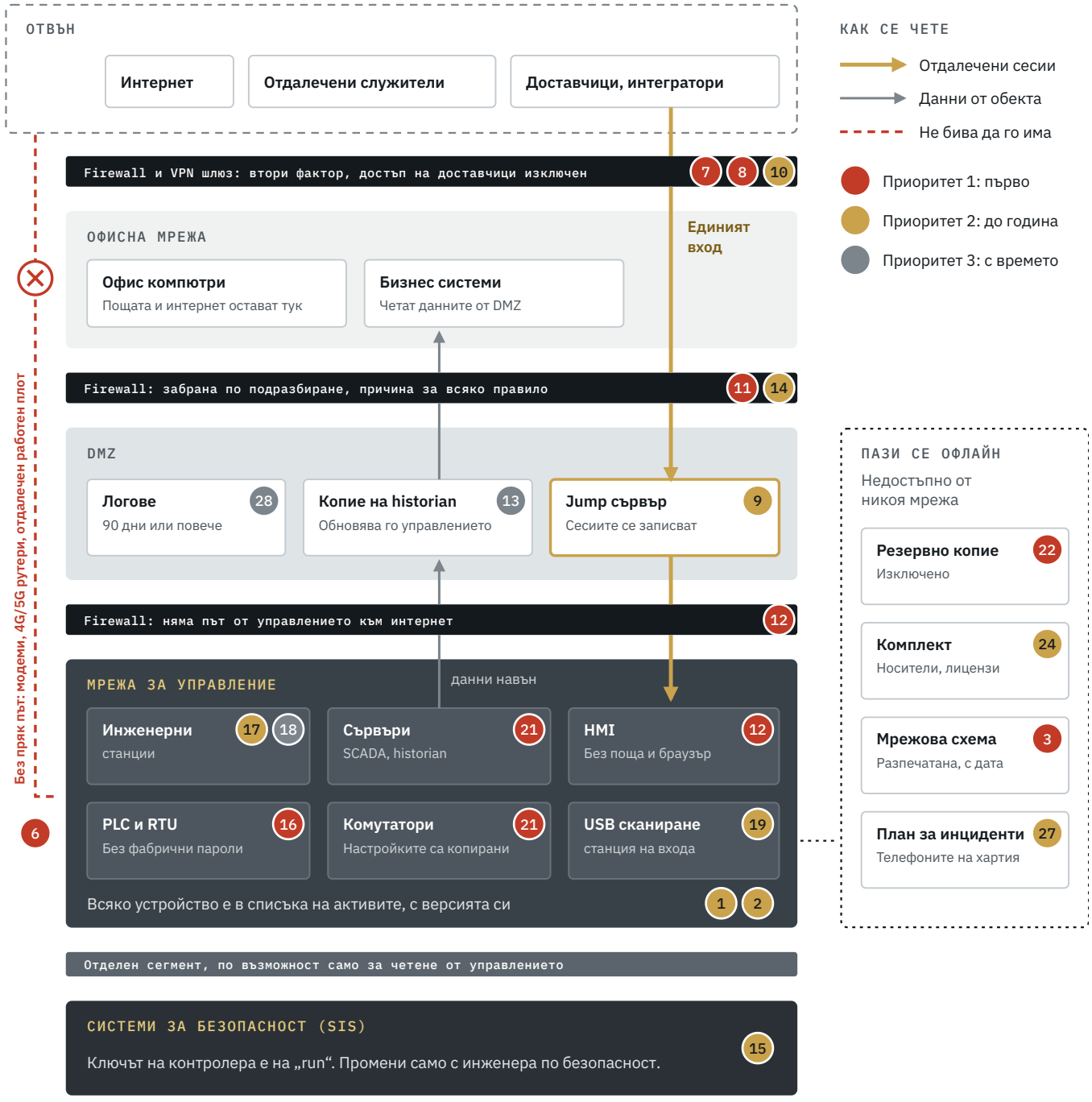
	ТОЧКА	ПРИОРИТЕТ	ДА	ОТЧАСТИ	НЕ	ДОКАЗАТЕЛСТВО
1	**Знайте какво управлявате**					
1	Списък на активите	П2	☐	☐	☐	
2	Версии в списъка	П2	☐	☐	☐	
3	Схема на мрежата	П1	☐	☐	☐	
4	Критични системи	П2	☐	☐	☐	
5	Бюлетини за сигурност от доставчиците	П2	☐	☐	☐	
2	**Отдалечен достъп**					
6	Всички входове отвън	П1	☐	☐	☐	
7	Втори фактор за отдалечения достъп	П1	☐	☐	☐	
8	Достъпът на доставчиците е изключен по подразбиране	П1	☐	☐	☐	
9	Една контролирана входна точка	П2	☐	☐	☐	
10	Преглед на отдалечените акаунти на три месеца	П2	☐	☐	☐	
3	**Разделяне на мрежите**					
11	Firewall между офиса и управлението	П1	☐	☐	☐	
12	Без интернет, поща и сърфиране на системите за управление	П1	☐	☐	☐	
13	Данните излизат през DMZ	П3	☐	☐	☐	
14	Годишен преглед на правилата на firewall-а	П2	☐	☐	☐	
15	Отделени системи за безопасност	П2	☐	☐	☐	
4	**Акаунти, пароли и устройства**					
16	Сменени пароли по подразбиране	П1	☐	☐	☐	
17	Лични акаунти	П2	☐	☐	☐	
18	Малко администратори	П3	☐	☐	☐	
19	Проверка на USB памети и външни лаптопи	П2	☐	☐	☐	
20	Напускащите губят достъп в последния си ден	П1	☐	☐	☐	
5	**Резервни копия и възстановяване**					
21	Резервни копия на това, което трябва на бизнеса	П1	☐	☐	☐	
22	Едно копие офлайн	П1	☐	☐	☐	
23	Изпробвано възстановяване	П1	☐	☐	☐	
24	Комплект за възстановяване офлайн	П2	☐	☐	☐	
25	Упражнена ръчна работа	П3	☐	☐	☐	
6	**Готовност за инциденти**					
26	Операторите познават признаците и знаят на кого да се обадят	П2	☐	☐	☐	
27	Кратък план за инциденти, телефоните и на хартия	П2	☐	☐	☐	
28	Логове, пазени 90 дни	П3	☐	☐	☐	
29	Кой докладва и ранното предупреждение до 24 часа	П2	☐	☐	☐	
30	Годишно учение	П3	☐	☐	☐	

Отговори „Да“ _____ от 30 **от които с Приоритет 1 _____ от 11** ДАТА _____

РАЗДЕЛИ 2 И 3 НА ЕДНА СХЕМА

Къде се прилагат точките

Един контролиран вход, firewall между всеки две зони и нищо, което да стига пряко до мрежата за управление. Числата са точките от списъка.



Извън схемата, защото са за хора и практика: 4 Критични системи · 5 Бюлетини за сигурност от доставчиците · 20 Напускащите губят достъп в последния си ден · 23 Изпробвано възстановяване · 25 Упражнена ръчна работа · 26 Операторите познават признаците и знаят на кого да се обадят · 29 Кой докладва и ранното предупреждение до 24 часа · 30 Годишно учение

РАЗДЕЛ 1 ОТ 6 / ТОЧКИ 1 ДО 5

1 Знайте какво управлявате

1 2 3 4 5

1 Списък на активите

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Имате списък на всеки PLC, RTU, HMI, инженерна станция и сървър в мрежата за управление, с местоположението му и с отговорника за него.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Не можете да защитите, обновите или възстановите оборудване, за което не знаете, че го имате. Всяка друга точка в този списък зависи от него.

КАК ИЗГЛЕЖДА ДОБРОТО

Една таблица или един инструмент с един отговорник. За всяко устройство: име, тип, производител и модел, местоположение (обект, шкаф), мрежов адрес, процесът, който обслужва, и отговорното лице.

КАК СЕ ПРАВИ

- Започнете от наличното: документацията на интегратора, проектните файлове на PLC, MAC таблиците на комутаторите, базата с тагове на SCADA.
- Обходете обекта със списъка, шкаф по шкаф. Записите на хартия винаги са остарели; обходът намира това, което те пропускат.
- Започнете с пасивно откриване в мрежата (слушане на трафика през огледален порт). Внимавайте с активното сканиране в работеща мрежа за управление: някои по-стари PLC и RTU спират или се рестартират при сканиране. За по-новите устройства активното сканиране с инструменти, създадени за ОТ, е възможност; скорошни изследвания показват, че то е по-малко опасно, отколкото се смяташе.
- Автоматизиран инструмент е за предпочитане, но таблица, която се обновява на всеки шест месеца, е по-добра от скъп инструмент, който никой не използва и не обновява.

КОЙ

Инженер по експлоатация или автоматизация, при нужда с интегратора.

ТРУД

3 до 10 дни за първата версия; след това по няколко часа на промяна.

ЧЕСТА ГРЕШКА

Списъкът се прави веднъж за одит и повече не се обновява. Добавете „обнови списъка на активите“ в процедурата за всяка промяна. Преглеждайте целия списък поне веднъж годишно.

2 Версии в списъка

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Списъкът показва версиите на фърмуера и софтуера и някой го е сверил с обекта през последните 12 месеца.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Когато производител обяви уязвимост, версиите ви казват за минути дали тя ви засяга, а не за седмици.

КАК ИЗГЛЕЖДА ДОБРОТО

Колона с версията на фърмуера и софтуера за всяко устройство, дата „последно проверено“ и годишна проверка.

КАК СЕ ПРАВИ

- Прочетете версиите от инженерния софтуер (повечето инструменти за PLC показват фърмуера при връзка с устройството) по време на планирана поддръжка.
- Запишете операционната система и нивото на обновленията за HMI, сървърите и инженерните станции.
- Отбележете дали производителят още поддържа устройството: устройствата без обновления за сигурност се нуждаят от допълнителна защита в мрежата (точки 11 и 14).

КОЙ

Инженер по автоматизация.

ТРУД

1 до 3 дни в допълнение към точка 1.

ЧЕСТА ГРЕШКА

Версията се записва веднъж при монтажа и повече не се обновява.

3 Схема на мрежата

ПРИОРИТЕТ 1 | ПЪРВО

Имате актуална схема на мрежата за управление, която показва всяка връзка с офисната мрежа, с интернет и с външни фирми.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Нападателите обикновено стигат до ОТ активите през връзка, за която никой не си е спомнил. Тази схема ви трябва за точки 6 и 11.

КАК ИЗГЛЕЖДА ДОБРОТО

Една схема, която показва зоните (офис, DMZ, управление, безопасност), всяка връзка между тях и всеки изход навън: firewall-и, VPN, модеми, 4G/5G рутери, връзки на доставчици, безжични връзки. С дата и с един отговорник.

КАК СЕ ПРАВИ

- Начертайте първо зоните, после връзките между тях. Подробностите вътре в зоната могат да дойдат по-късно.
- Потвърдете всяка връзка физически: проследете кабелите, проверете настройките на firewall-а и рутера, потърсете 4G/5G рутери в шкафовете.
- Отбележете собственика и целта на всяка външна връзка. Връзка без собственик и без цел е кандидат за премахване.
- Пазете разпечатано копие офлайн. Ще ви трябва по време на инцидент.

КОЙ

Инженер по автоматизация заедно с мрежовите специалисти от ИТ.

ТРУД

2 до 5 дни.

ЧЕСТА ГРЕШКА

Схема на това как е била проектирана мрежата, без потоците от данни и без собствениците на външните връзки.

4 Критични системи

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Знаете без кои системи процесът не може да работи повече от няколко часа. ☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Тези системи получават най-силната защита и най-добрите резервни копия и ги възстановявате първи.

КАК ИЗГЛЕЖДА ДОБРОТО

Кратък списък (често 5 до 15 системи), който показва за всяка колко дълго процесът може да работи без нея и какво става, когато тя спре.

КАК СЕ ПРАВИ

- Проведете двучасова работна среща с експлоатацията, поддръжката и ръководителя на обекта. Питайте: „Ако тази система спре сега, какво става след един час, един ден, една седмица?“
- Отбележете критичните системи в списъка на активите и на схемата.
- Използвайте резултата, за да подредите плана за възстановяване (точка 23) и работата по защитата.

КОЙ

Ръководителят на обекта и ръководителят на експлоатацията.

ТРУД

1 до 2 дни заедно с работната среща.

ЧЕСТА ГРЕШКА

Всичко се отбелязва като критично. Ако всичко е критично, нищо не е.

5 Бюлетини за сигурност от доставчиците

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Определен човек получава бюлетините за сигурност от доставчиците на оборудването ви и решава какво да се направи с всеки от тях. ☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Бюлетин, който никой не чете, е известна уязвимост, която остава отворена, и възможен вход за нападателите.

КАК ИЗГЛЕЖДА ДОБРОТО

Определен човек, абонамент за известията за сигурност на всеки доставчик и за публичен източник на бюлетини за индустриални системи. Също и кратък запис за всеки бюлетин: засяга ли ни (да/не, според списъка на активите), решение, дата.

КАК СЕ ПРАВИ

- Абонирайте се за известията за сигурност на всеки основен доставчик.
- Сверявайте всеки бюлетин със списъка на активите (точка 2).
- Изберете едно от четири действия: обновяване при следващото планирано спиране, допълнителна защита в мрежата вместо това, приемане на риска с обосновка или „не ни засяга“. Запишете решението.
- В ОТ обновяването рядко е незабавно. Документирано решение с компенсираща мярка често е верният отговор.

КОЙ

Инженер по автоматизация или отговорникът за ОТ сигурността.

ТРУД

1 ден за настройка; след това 1 до 2 часа на месец.

ЧЕСТА ГРЕШКА

Бюлетините се пренебрегват или обновленията се инсталират веднага, без проверка. Изпробвайте заедно с доставчика или на резервна система и обновявайте по време на планирана поддръжка.

РАЗДЕЛ 2 ОТ 6 / ТОЧКИ 6 ДО 10

2 Отдалечен достъп

6 7 8 9 10

6 Всички входове отвън

ПРИОРИТЕТ 1 | ПЪРВО

Можете да изброите всеки вход отвън към мрежата за управление: VPN, инструменти за отдалечен работен плот, модеми на доставчици и 4G/5G рутери.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Забравен модем или инструмент за отдалечен работен плот е един от най-честите входове.

КАК ИЗГЛЕЖДА ДОБРОТО

Пълен списък на пътищата за отдалечен достъп, всеки със собственик, група потребители, цел и одобрение.

КАК СЕ ПРАВИ

- Използвайте схемата (точка 3) и попитайте всеки доставчик и интегратор как се свързва днес.
- Потърсете инсталирани инструменти за отдалечен работен плот на HMI, сървърите и инженерните станции.
- Проверете на място шкафовете и диспечерските зали за модеми и 4G/5G рутери.
- Премахнете всеки път, който не можете да обосновете. Останалите преместете към едната контролирана входна точка (точка 9).

КОЙ

Инженер по автоматизация заедно с ИТ сигурността.

ТРУД

2 до 5 дни.

ЧЕСТА ГРЕШКА

Доверие в документите. Вредят ви точно пътищата, които никой не е записал.

7 Втори фактор за отдалечения достъп

ПРИОРИТЕТ 1 | ПЪРВО

Всяка отдалечена връзка към мрежата за управление изисква втори фактор, например код от телефон или хардуерен ключ.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

С втори фактор откраднатата парола сама не е достатъчна. Откраднати или отгатнати пароли стоят зад голяма част от инцидентите със сигурността.

КАК ИЗГЛЕЖДА ДОБРОТО

Двуфакторно удостоверяване за всеки VPN и за всеки акаунт за отдалечен достъп, включително на доставчиците, без изключения за „служебни“ акаунти.

КАК СЕ ПРАВИ

- Включете го на входната точка (VPN или шлюз за отдалечен достъп), за да обхване всички, които влизат оттам.
- Дайте на доставчиците лични акаунти с втори фактор. Без общи акаунти за доставчика.
- Предпочитайте приложение или хардуерен ключ пред кодове по SMS.
- Помислете за нощната смяна: работещ ред при изгубен телефон, за да не изключи никой втория фактор „временно“.

КОЙ

ИТ сигурността, а внедряването заедно с експлоатацията.

ТРУД

2 до 5 дни, често със съществуващите VPN лицензи.

ЧЕСТА ГРЕШКА

Един общ акаунт „доставчик“, чийто втори фактор е на телефона на един човек.

8 Достъпът на доставчиците е изключен по подразбиране

ПРИОРИТЕТ 1 | ПЪРВО

Достъпът на доставчиците и интеграторите е изключен по подразбиране. Включвате го за конкретна задача и го изключвате, когато тя приключи.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Достъп, който е винаги включен, е достъп, който и нападател може да използва в 3 часа през нощта.

КАК ИЗГЛЕЖДА ДОБРОТО

Акаунтите на доставчиците са деактивирани по подразбиране. Кратък ред за заявка: кой, към коя система, защо и за колко време. Достъпът се отваря от ваш служител и се затваря, когато задачата приключи или в края на деня.

КАК СЕ ПРАВИ

- Деактивирайте всички акаунти на доставчици сега. Активирайте ги при заявка с основателна причина.
- Използвайте проста форма за заявка или тикет. Одобрява диспечерската зала.
- Където инструментите позволяват, задайте достъпът да изтича автоматично.
- За критичните системи записвайте или наблюдавайте действията.

КОЙ

Ръководителят на експлоатацията (одобрява), ИТ или автоматизацията (отварят и затварят).

ТРУД

1 до 2 дни за настройка.

ЧЕСТА ГРЕШКА

Изключение по спешност, което става постоянно.

9 Една контролирана входна точка

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Отдалечените сесии минават през една контролирана точка, например jump сървър (bastion host), където се записват в логове. Никой не се свързва отвън направо към PLC или HMI.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Една входна точка е едно място за наблюдение, а с включени логове виждате кой какво е направил.

КАК ИЗГЛЕЖДА ДОБРОТО

Jump сървър или шлюз за отдалечен достъп в DMZ. Потребителите се свързват към него, а оттам към целта. Сесиите се записват в логове, а за доставчиците по възможност се записват изцяло.

КАК СЕ ПРАВИ

- Поставете jump сървъра в DMZ (точка 13), а не в мрежата за управление.
- Инсталирайте на jump сървъра инженерните инструменти, които трябват на доставчиците, за да не носят свой лаптоп.
- Разрешете трафик от jump сървъра само към системите, които трябват на всеки потребител.
- Пазете логовете му там, където нападател не може лесно да ги изтрие (точка 28).

КОЙ

ИТ сигурността заедно с инженерите по автоматизация.

ТРУД

5 до 15 дни, плюс хардуер или лицензи.

ЧЕСТА ГРЕШКА

Jump сървър с пряк път покрай него, който е „само за спешни случаи“.

10 Преглед на отдалечените акаунти на три месеца

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Поне на всеки три месеца някой преглежда акаунтите за отдалечен достъп и премахва ненужните.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Старите акаунти на бивши служители и на приключили проекти са лесна мишена.

КАК ИЗГЛЕЖДА ДОБРОТО

Запис с дата за всяко тримесечие: списък на акаунтите, остава или се премахва, и кой е решил.

КАК СЕ ПРАВИ

- Изведете списъка на акаунтите от VPN или шлюза.
- Изпратете го на ръководителя на експлоатацията, за да потвърди всеки акаунт.
- Деактивирайте това, което никой не потвърди. Ако на някого му трябва, ще поиска.
- Пазете записа. Това е доказателството, което одиторът иска.

КОЙ

ИТ сигурността заедно с ръководителя на експлоатацията.

ТРУД

2 до 4 часа на тримесечие.

ЧЕСТА ГРЕШКА

Преглед, след който нищо не се премахва.

3 Разделяне на мрежите

РАЗДЕЛ 3 ОТ 6 / ТОЧКИ 11 ДО 15

11 12 13 14 15

11 Firewall между офиса и управлението

ПРИОРИТЕТ 1 | ПЪРВО

Firewall отделя мрежата за управление от офисната мрежа и всяко негово правило има записана причина.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Ако рансъмуер удари офиса, firewall-ът решава дали той ще стигне до производството.

КАК ИЗГЛЕЖДА ДОБРОТО

Отделен firewall (а не само рутер или VLAN) между офиса и управлението. Правило по подразбиране: забрана. Всяко разрешаващо правило има източник, цел, порт, причина и собственик.

КАК СЕ ПРАВИ

- Ако няма firewall, това е първата покупка.
- Преди да затегнете правилата, наблюдавайте трафика две до четири седмици, за да разберете какво наистина трябва на процеса.
- Въведете забраната на стъпки, по време на планирана поддръжка, с план за връщане назад.
- Запишете причината до всяко правило в самия firewall.

КОЙ

Мрежовите специалисти от ИТ заедно с инженерите по автоматизация.

ТРУД

5 до 15 дни, плюс хардуер при нужда.

ЧЕСТА ГРЕШКА

VLAN без филтриране, наречен „сегментиране“.

12 Без интернет, поща и сърфиране на системите за управление

ПРИОРИТЕТ 1 | ПЪРВО

Никоя система за управление няма пряк достъп до интернет и никой не чете поща и не сърфира от HMI или инженерна станция.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Електронната поща и сърфирането са пътят, по който идва повечето зловреден софтуер.

КАК ИЗГЛЕЖДА ДОБРОТО

Firewall-ът спира изходящия интернет от мрежата за управление. На HMI и инженерните станции няма пощенски клиент и не се използва браузър. Обновленията идват по контролиран път.

КАК СЕ ПРАВИ

- Спрете изходящия интернет на firewall-а и вижте в логовете какво спира да работи. Обикновено е проверка на лиценз или услуга за обновления; дайте им тесен, документиран път.
- Дайте на операторите и инженерите отделен офис компютър за поща и интернет.
- Внасяйте обновленията през DMZ или с проверени USB памети (точка 19).

КОЙ

Мрежовите специалисти от ИТ заедно с експлоатацията.

ТРУД

2 до 5 дни.

ЧЕСТА ГРЕШКА

Правила „само за този един лицензен сървър“, които отварят много повече от нужното.

13 Данните излизат през DMZ

ПРИОРИТЕТ 3 | С ВРЕМЕТО

Данните, които трябват на бизнеса, например данни от historian и отчети, излизат от мрежата за управление през отделна зона (DMZ), а не през пряка връзка.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Така офисът никога не се нуждае от пряк път към мрежата за управление и нападателят няма пряка връзка, с която да злоупотреби.

КАК ИЗГЛЕЖДА ДОБРОТО

DMZ между офиса и управлението. Страната на управлението изпраща данните към копие на historian или файлов сървър в DMZ. Офисът чете от DMZ. Няма пряка връзка от офиса към управлението.

КАК СЕ ПРАВИ

- Проектирайте това заедно с точка 11; често е един проект.
- Започнете с historian: копие в DMZ, което се обновява от страната на управлението.
- Преместете jump сървъра (точка 9) и услугите за обновления в DMZ.
- За много критични обекти помислете за еднопосочен диод за данните, които само трябва да излизат.

КОЙ

Мрежовите специалисти от ИТ, инженерите по автоматизация и отговорникът за historian.

ТРУД

10 до 30 дни, плюс хардуер. Често е планиран проект.

ЧЕСТА ГРЕШКА

DMZ, която офисът все още може да заобиколи.

14 Годишен преглед на правилата на firewall-а

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

През последните 12 месеца някой е прегледал правилата на firewall-а и е премахнал тези, които разрешават целия трафик.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Временните правила за една задача обикновено остават с години.

КАК ИЗГЛЕЖДА ДОБРОТО

Запис от годишен преглед. Няма правила „от всички към всички“. Всяко правило има причина и собственик, а временните правила имат крайна дата.

КАК СЕ ПРАВИ

- Изведете правилата и броя на съвпаденията им. Правилата без съвпадения за 90 дни са кандидати за премахване.
- Попитайте собственика на всяко правило дали то още е нужно.
- Премахвайте на стъпки, по време на планирана поддръжка, с план за връщане назад.

КОЙ

Мрежовите специалисти от ИТ заедно с инженерите по автоматизация.

ТРУД

1 до 3 дни годишно.

ЧЕСТА ГРЕШКА

Страх да се премахне каквото и да е, затова нищо не се променя.

15 Отделени системи за безопасност

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Системите за безопасност (SIS) са в собствен мрежов сегмент или са физически отделени от системата за управление.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Атака срещу системата за управление не бива да може да изключи защитата.

КАК ИЗГЛЕЖДА ДОБРОТО

SIS е в собствена зона, само с връзките, които изисква обосновката на безопасността, по възможност само за четене от страната на управлението. Ключът за режима на контролера на SIS е на „run“, а не на „program“.

КАК СЕ ПРАВИ

- Проверете на схемата всяка връзка към SIS. Премахнете това, което не е нужно за безопасността.
- Дръжте контролера на SIS в режим „run“; минавайте на „program“ само с наряд.
- Съгласувайте промените с инженера си по безопасност и спазвайте процеса си за функционална безопасност (IEC 61511). Никога не променяйте връзка към SIS без него.

КОЙ

Инженерът по безопасност и инженерът по автоматизация.

ТРУД

2 до 10 дни, според проекта.

ЧЕСТА ГРЕШКА

Инженерна станция, която достига и системата за управление, и SIS, оставена с влязъл потребител.

РАЗДЕЛ 4 ОТ 6 / ТОЧКИ 16 ДО 20

4 Акаунти, пароли и устройства

16 17 18 19 20

16 Сменени пароли по подразбиране

ПРИОРИТЕТ 1 | ПЪРВО

Паролите по подразбиране на PLC, HMI, комутаторите и firewall-ите са сменени.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Паролите по подразбиране са публикувани в ръководствата на самите производители.

КАК ИЗГЛЕЖДА ДОБРОТО

Никъде в мрежата за управление няма парола по подразбиране. Новите пароли се пазят в хранилище за пароли или в запечатан запис, а не на бележка върху шкафа.

КАК СЕ ПРАВИ

- Използвайте списъка на активите (точка 1) и минете устройство по устройство.
- Където устройството не позволява смяна на паролата, защитете го в мрежата (точки 11 и 14) и запишете изключението.
- Сменяйте паролите по време на планирана поддръжка; някои устройства изискват рестарт или зареждане на проекта.
- Пазете новите пароли в хранилище за пароли с достъп за хората, на които трябват, и запечатано копие за спешни случаи.

КОЙ

Инженер по автоматизация.

ТРУД

2 до 5 дни.

ЧЕСТА ГРЕШКА

Една и съща нова парола на всяко устройство.

17 Лични акаунти

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Всеки човек има собствен акаунт. Общи акаунти се използват само там, където системата не позволява друго, и паролите им се сменят, когато някой напусне.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

С лични акаунти знаете кой е направил промяната и можете да отнемете достъпа на един човек.

КАК ИЗГЛЕЖДА ДОБРОТО

Лични акаунти на инженерните станции, сървърите, jump сървъра и VPN. Общ операторски акаунт на HMI е приемлив там, където HMI го изисква, със списък на хората, които знаят паролата.

КАК СЕ ПРАВИ

- Започнете оттам, където е най-лесно: VPN, jump сървър, сървъри, инженерни станции.
- За HMI запазете общия операторски акаунт, ако личното влизане би забавило операторите; защитете инженерните функции с лични акаунти.
- Водете списък на всеки общ акаунт и на хората, които знаят паролата му.

КОЙ

ИТ заедно с инженерите по автоматизация.

ТРУД

3 до 10 дни.

ЧЕСТА ГРЕШКА

Работата на операторите става по-трудна. Сигурност, която бави диспечерската зала, бива изключена до месец.

18 Малко администратори

ПРИОРИТЕТ 3 | С ВРЕМЕТО

Само хората, на които е нужно, имат администраторски права на инженерните станции и сървърите.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

По-малко администратори означава по-малко акаунти, с които нападател може да промени процеса.

КАК ИЗГЛЕЖДА ДОБРОТО

Кратък списък на администраторите, който се преглежда заедно с точка 10. Всекидневната работа е с обикновен акаунт.

КАК СЕ ПРАВИ

- Изброете кой има администраторски права сега.
- Отнемете правата от всекидневните акаунти. На хората, на които трябват, дайте отделен администраторски акаунт.
- Преди да отнемете правата, проверете дали инженерният софтуер работи без тях; някои по-стари инструменти изискват изключения.

КОЙ

ИТ заедно с инженерите по автоматизация.

ТРУД

1 до 3 дни.

ЧЕСТА ГРЕШКА

Правата се отнемат, без да са изпробвани инженерните инструменти.

19 Проверка на USB памети и външни лаптопи

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

USB паметите и лаптопите, внесени на обекта, се проверяват, преди да се свържат към система за управление, например на станция за сканиране.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Мрежи, които са отделени от интернет, пак се заразяват през USB памети и лаптопи на посетители.

КАК ИЗГЛЕЖДА ДОБРОТО

Станция за сканиране на входа на диспечерската зала. Правило всяка USB памет да се сканира преди употреба. Лаптопите на доставчиците или се сканират, или не се свързват; вместо това доставчиците работят през jump сървъра.

КАК СЕ ПРАВИ

- Направете станция за сканиране (отделен компютър с актуална защита от зловреден софтуер, по възможност с повече от един скенер).
- Дайте на служителите фирмени USB памети, които остават на обекта.
- Забранете USB паметите на HMI и инженерните станции, където процесът го позволява.
- Информирайте доставчиците преди посещението им. Правилото се спазва по-лесно, когато го очакват.

КОЙ

Ръководителят на експлоатацията заедно с ИТ сигурността.

ТРУД

2 до 5 дни.

ЧЕСТА ГРЕШКА

Станция за сканиране, която никой не използва, защото е на неудобно място.

20 Напускащите губят достъп в последния си ден

ПРИОРИТЕТ 1 | ПЪРВО

Служителите и външните изпълнители, които напускат, губят целия си достъп, включително отдалечения, в последния си работен ден.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Достъпът на напусналите рядко се наблюдава от някого.

КАК ИЗГЛЕЖДА ДОБРОТО

Списък за напускане, който включва акаунтите в системите за управление, VPN, jump сървъра, общите пароли, които човекът е знаел, и физическите ключове или карти.

КАК СЕ ПРАВИ

- Добавете акаунтите в системите за управление към процеса на „Човешки ресурси“ при напускане.
- Сменете общите пароли, които напускащият е знаел (точка 17).
- За външните изпълнители ръководителят на проекта потвърждава крайната дата и акаунтите изтичат на тази дата.

КОЙ

„Човешки ресурси“, ИТ и ръководителят на експлоатацията.

ТРУД

1 ден за настройка.

ЧЕСТА ГРЕШКА

Процесът при напускане обхваща само офисните ИТ системи, но не и производството.

5 Резервни копия и възстановяване

РАЗДЕЛ 5 ОТ 6 / ТОЧКИ 21 ДО 25

21 22 23 24 25

21 Резервни копия на това, което трябва на бизнеса

ПРИОРИТЕТ 1 | ПЪРВО

Имате актуални резервни копия на програмите на PLC, проектите на HMI, настройките на комутаторите и firewall-ите и образи на инженерните станции.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Без програмите на PLC и проектите на HMI възстановяването отнема седмици вместо дни.

КАК ИЗГЛЕЖДА ДОБРОТО

Резервно копие за всяка критична система (точка 4), направено след всяка промяна и поне на всяко тримесечие, с дата, версия и името на човека, който го е направил.

КАК СЕ ПРАВИ

- Започнете с критичните системи.
- Вземете програмата на PLC от работещия контролер, а не от лаптопа на интегратора; често се различават.
- Направете копие и на настройките на мрежовите устройства и на правилата на firewall-а.
- Направете „вземи резервно копие“ последната стъпка от всяка промяна.

КОЙ

Инженер по автоматизация.

ТРУД

3 до 10 дни за първия пълен комплект.

ЧЕСТА ГРЕШКА

Единственото копие на програмата на PLC е на лаптопа на интегратора.

22 Едно копие офлайн

ПРИОРИТЕТ 1 | ПЪРВО

Поне едно от тези резервни копия се пази офлайн или извън мрежата за управление.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Рансъмуерът криптира всяко резервно копие, до което може да стигне.

КАК ИЗГЛЕЖДА ДОБРОТО

Три копия на два вида носители, едното офлайн или на друго място. Офлайн копието се обновява след всяка промяна и поне на всяко тримесечие.

КАК СЕ ПРАВИ

- Копирайте резервните копия на външен диск или защитено хранилище, което се изключва след всяко обновяване.
- Пазете едно копие на друг обект или в огнеупорна каса.
- Защитете офлайн копието с криптиране и запишете кой държи ключа.

КОЙ

Инженер по автоматизация заедно с ИТ.

ТРУД

1 до 2 дни за настройка.

ЧЕСТА ГРЕШКА

Диск с резервни копия, който остава свързан „за удобство“.

23 Изпробвано възстановяване

ПРИОРИТЕТ 1 | ПЪРВО

През последните 12 месеца някой е възстановил система от резервно копие и е видял, че тя работи.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Резервното копие е доказано едва когато възстановяването от него е успяло.

КАК ИЗГЛЕЖДА ДОБРОТО

Годишен тест за възстановяване на всяка критична система, с кратък запис: какво е възстановено, колко време е отнело и какво е липсвало.

КАК СЕ ПРАВИ

- Възстановявайте на резервен контролер или тестов компютър, а не на работещата система.
- Измерете времето за възстановяване. То ви казва дали точка 25 е реалистична.
- Запишете всичко, което е липсвало (лицензи, драйвери, пароли), и го оправете.
- Започнете с една критична система; добавяйте по една на тримесечие.

КОЙ

Инженер по автоматизация.

ТРУД

1 до 2 дни на система.

ЧЕСТА ГРЕШКА

Проверява се дали файлът с резервното копие съществува, а не дали се възстановява.

24 Комплект за възстановяване офлайн

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Инсталационните носители, лицензите и проектните файлове за възстановяване на инженерна станция се пазят там, където можете да ги намерите без мрежата.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

По време на инцидент мрежата и файловият сървър може да са първото, което ще загубите.

КАК ИЗГЛЕЖДА ДОБРОТО

„Комплект за възстановяване“ за всяка критична система: инсталационни носители, лицензни ключове или хардуерни ключове (донгъли), проектни файлове и кратка инструкция за възстановяване, всичко офлайн.

КАК СЕ ПРАВИ

- Съберете комплекта по време на първия тест за възстановяване (точка 23); тестът показва какво ви трябва.
- Попитайте доставчиците как се възстановяват лицензите без достъп до интернет.
- Пазете един комплект на обекта и един на друго място.

КОЙ

Инженер по автоматизация.

ТРУД

1 до 3 дни.

ЧЕСТА ГРЕШКА

Лиценз, който може да се активира само онлайн.

25 Упражнена ръчна работа

ПРИОРИТЕТ 3 | С ВРЕМЕТО

Знаете колко дълго можете да водите процеса ръчно или да го държите в безопасно състояние и операторите са го упражнявали.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Това е времето, с което разполагате, за да възстановите системите за управление.

КАК ИЗГЛЕЖДА ДОБРОТО

Писмена процедура за ръчна или ограничена работа и за безопасно спиране. Операторите я упражняват веднъж годишно. Времето, което тя издържа, е известно и е сравнено с времената за възстановяване от точка 23.

КАК СЕ ПРАВИ

- Напишете процедурата заедно с най-опитните оператори.
- Упражнявайте в планиран период на ниско натоварване.
- Сравнете: ако ръчната работа издържа 8 часа, а възстановяването отнема 3 дни, ви трябва по-добър план.

КОЙ

Ръководителят на експлоатацията и ръководителят на обекта.

ТРУД

2 до 5 дни плюс упражнението.

ЧЕСТА ГРЕШКА

Приема се, че старите умения за ръчна работа още ги има.

РАЗДЕЛ 6 ОТ 6 / ТОЧКИ 26 ДО 30

6 Готовност за инциденти

26 27 28 29 30

26 Операторите познават признаците и знаят на кого да се обадят

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Операторите знаят какво изглежда нередно, например HMI, който се движи сам, непознати влизания или променени задания, и на кого да се обадят по всяко време.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Операторът на смяна обикновено е първият човек, който вижда атаката.

КАК ИЗГЛЕЖДА ДОБРОТО

Карта от една страница в диспечерската зала: признаците, първите три действия и телефонните номера. Кратък инструктаж за всяка смяна веднъж годишно.

КАК СЕ ПРАВИ

- Напишете картата заедно с операторите, с техните думи.
- Първи действия: не изключвайте нищо, освен ако безопасността не го изисква; запишете какво виждате и кога; обадете се на номера.
- Инструктирайте всяка смяна веднъж годишно, заедно с инструктажа по безопасност. Петнадесет минути стигат.

КОЙ

Ръководителят на експлоатацията.

ТРУД

1 до 2 дни.

ЧЕСТА ГРЕШКА

Процедура за киберинциденти, която разбират само в ИТ.

27 Кратък план за инциденти, телефоните и на хартия

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Има кратък писмен план за инциденти в средата за управление, а телефонните номера са и на хартия.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

При инцидент системите, в които са планът и номерата, може да не работят.

КАК ИЗГЛЕЖДА ДОБРОТО

План от няколко страници: кой решава, на кого се звъни (вътрешни хора, доставчици, компетентен орган, застраховател), кога мрежата за управление се изолира от офиса и как процесът остава безопасен. Разпечатан, в диспечерската зала.

КАК СЕ ПРАВИ

- Нека е кратък. План, който никой не чете, не помага.
- Определете предварително кой може да реши обектът да се изключи от офисната мрежа, за да не чака никой разрешение.
- Включете спешните номера на основните си доставчици и на застрахователя.
- Преглеждайте го след всяко учение (точка 30).

КОЙ

Отговорникът за ОТ сигурността заедно с експлоатацията и ръководството.

ТРУД

3 до 5 дни.

ЧЕСТА ГРЕШКА

Копие на ИТ плана за инциденти, към което е добавено „ОТ“.

28 Логове, пазени 90 дни

ПРИОРИТЕТ 3 | С ВРЕМЕТО

Логовете от firewall-ите, отдалечения достъп и ключовите сървъри се пазят поне 90 дни, там, където нападател не може лесно да ги изтрие.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Нападателите често са вътре седмици, преди някой да забележи, а логовете показват как са влезли.

КАК ИЗГЛЕЖДА ДОБРОТО

Логовете от firewall-ите, VPN, jump сървъра и Windows сървърите се изпращат в едно централно хранилище, пазят се 90 дни или повече и някой следи важните сигнали.

КАК СЕ ПРАВИ

- Започнете с най-важните логове: firewall, VPN, jump сървър.
- Изпращайте ги в централно хранилище извън мрежата за управление.
- Проверете часовниците: всички системи трябва да са на едно и също време, иначе логовете не могат да се сравняват.
- По-късно помислете за инструмент за наблюдение на ОТ мрежата. Направете го след Приоритет 1 и 2, не преди това.

КОЙ

ИТ сигурността.

ТРУД

3 до 10 дни.

ЧЕСТА ГРЕШКА

Купува се инструмент за наблюдение, преди основите да са налице, и никой не гледа сигналите му.

29 Кой докладва и ранното предупреждение до 24 часа

ПРИОРИТЕТ 2 | ТАЗИ ГОДИНА

Знаете кой докладва сериозен инцидент на компетентния орган и че NIS2 изисква ранно предупреждение до 24 часа.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

24 часа минават бързо, когато сте заети да спасявате работата на обекта.

КАК ИЗГЛЕЖДА ДОБРОТО

Определен човек и заместник. Данните за контакт с националния CSIRT или компетентния орган са в плана за инциденти. Готов кратък образец. Според NIS2: ранно предупреждение до 24 часа, уведомление за инцидента до 72 часа и окончателен доклад до един месец.

КАК СЕ ПРАВИ

- Разберете кой орган отговаря за вашия сектор и как приема докладите.
- Подгответе образец за ранното предупреждение; може да е кратък.
- Определете предварително кой може да го изпрати, за да не чака управителния орган.
- Упражнете го в ученията (точка 30).

КОЙ

Отговорникът за ОТ сигурността, ръководството и юристите.

ТРУД

1 до 2 дни.

ЧЕСТА ГРЕШКА

Смята се, че 24-те часа започват след разследването. Те започват, когато узнаете за значителен инцидент.

30 Годишно учение

ПРИОРИТЕТ 3 | С ВРЕМЕТО

През последните 12 месеца експлоатацията и ръководството са провели учение за киберинцидент на обекта, дори да е било само двучасово обсъждане на маса.

☐ ДА ☐ ОТЧАСТИ ☐ НЕ

ЗАЩО

Учението показва пропуските в плана, преди да го направи истински инцидент.

КАК ИЗГЛЕЖДА ДОБРОТО

Годишно tabletop учение с експлоатацията, ИТ, ръководството и по възможност ключов доставчик. Кратък списък с изводи, със собственици и срокове.

КАК СЕ ПРАВИ

- Използвайте реалистичен сценарий: рансъмуер в офиса, който се разпространява към производството, или акаунт на доставчик, използван през нощта.
- Два до три часа стигат. Нека го води човек извън екипа.
- Включете решението за изолиране, безопасното състояние и доклада до 24 часа.
- Запишете изводите, дайте на всеки собственик и срок и ги проверете на следващото учение.

КОЙ

Отговорникът за ОТ сигурността заедно с ръководството.

ТРУД

2 до 3 дни подготовка, плюс учението.

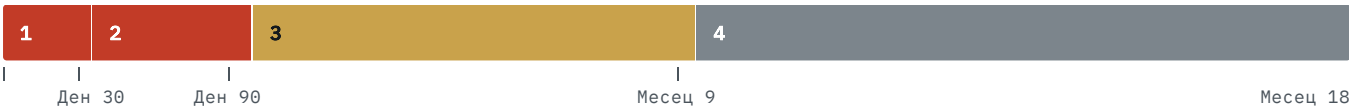
ЧЕСТА ГРЕШКА

Толкова лесен сценарий, че никой не научава нищо.

ПЛАНЪТ

Реалистичен ред

От първите 30 дни до 18-ия месец. Първите две фази са кратки нарочно: те затварят преките входове и доказват, че можете да се възстановите.



1 Вижте и затворете вратите

ДНИ 1 ДО 30 · ПРИОРИТЕТ 1

- 3 Схема на мрежата
- 8 Достъпът на доставчиците е изключен
- 16 Пароли по подразбиране (започнете с критичните системи)
- 6 Всички входове
- 20 Процес при напускане

2 Заключете вратите и осигурете пътя назад

ДНИ 30 ДО 90 · ПРИОРИТЕТ 1

- 7 Втори фактор
- 12 Без интернет на системите за управление
- 22 Офлайн копие
- 11 Firewall офис/управление
- 21 Резервни копия
- 23 Първи тест за възстановяване

3 Направете го трайно и доказуемо

МЕСЕЦИ 3 ДО 9 · ПРИОРИТЕТ 2

- 1 Списък на активите
- 5 Бюлетини
- 14 Преглед на firewall-а
- 19 USB процес
- 27 План за инциденти
- 2 Версии
- 9 Jump сървър
- 15 Отделяне на безопасността
- 24 Комплект за възстановяване
- 29 Докладване
- 4 Критични системи
- 10 Преглед на акаунтите
- 17 Лични акаунти
- 26 Карта за операторите

4 Изградете зрялост

МЕСЕЦИ 9 ДО 18 · ПРИОРИТЕТ 3

- 13 DMZ
- 25 Упражнена ръчна работа
- 30 Годишно учение
- 18 Малко администратори
- 28 Централни логове

Бележка. Точки 1 и 3 се подкрепят. Груба схема в началото (Приоритет 1) ви позволява бързо да затворите вратите; пълният списък на активите (Приоритет 2) след това прави всичко останало по-лесно за поддържане.

СЛЕД ТОЗИ ЧАС

Вашият резултат

☐ **Отговори „Да“** от 30	☐ **Отговори „Да“ с Приоритет 1** от 11

0 до 12
Изложени

Вероятно има отворени преки входове, а възстановяването не е доказано. Започнете точките с Приоритет 1 още този месец.

13 до 22
Основите са налице

Главните врати са затворени. Минете през Приоритет 2, за да се задържат основите и да можете да покажете доказателствата.

23 до 30
Добре подготвени

Продължавайте прегледите и учението и нека външен човек провери това, в което вярвате.

> **Едно правило над резултата.** „Не“ на която и да е точка с Приоритет 1 е първа задача, какъвто и да е общият ви брой.

Вашите три първи действия

Започнете с точките с Приоритет 1, на които сте отговорили с „Не“.

1 _____

2 _____

3 _____

Следващи стъпки

Проверка на готовността за NIS2

Безплатна, около пет минути. Обхваща управленската страна, например одобрение от ръководството, оценка на риска, доставчици и докладване, и ви изпраща личен доклад по имейл.

kimk-t.com/bg/nis2-readiness

30-минутен разговор

Минете през отговорите си с Иван Драгнев. Без търговска презентация.

kimk-t.com/bg/book

KIMK

OFFICE@KIMK-T.COM / KIMK-T.COM/BG