ЗА ПОТЕНЦИАЛНИТЕ ПРОПУСКИ, РИСКОВЕ И ЗАПЛАХИ В ЗАЩИТАТА НА ИНДУСТРИАЛНИТЕ СИСТЕМИ.

НЕОБХОДИМИ МЕРКИ ЗА СИГУРНОСТ, ПЛАНИРАНЕ НА КРАТКОСРОЧНИ И ДЪЛГОСРОЧНИ ДЕЙСТВИЯ ЗА ПОДОБРЯВАНЕ НА КИБЕР СИГУРНОСТТА НА ICS / SCADA СИСТЕМИТЕ.

Предоставено от:

Й.Ж. ISO/IEC 27001:2013 LA, ISO/IEC 20000-1:2011 IA 02.10.2018

В материала: преглед на потенциалните заплахи и пропуски в информационната инфраструктура, организацията на достъпите и позволенията, насочващи аналитични позиции и предложения за подобряване на сигурността на ICS/ SCADA за индустриални(производствени) фирми и предприятия. Предоставени са няколко конкретни стъпки с описани действия за минимизиране и избягване на кибер инциденти, стъпки, които ще подпомогнат изграждането на работеща документална и процедурна база относно кибер сигурността на ICS / SCADA.

Предварително уточнение: предоставените препоръки целят да подпомогнат фирмите и/или заинтересованите субекти да направят своя критичен анализ на текущо състояние на производствените системи, чрез което да се върви към повишаване на кибер сигурността в производствените организации. Няколко са основните цели: -превенция с ясни, конкретни проактивни действия – т.е. задълбочено познаване структурата и организацията на производствената система и постоянен проактивен анализ; -постоянни активни действия, наблюдение и контрол на ICS / SCADA; -намаляване, избягване на реактивните действия по отношение на сигурността на ICS / SCADA; при действия на реакция да се сведат до минимум (да се ограничат) загубите и времето за възстановяване на производствените системи; -задължителен пост реактивен задълбочен анализ на коренните причини с последващи ефективни коригиращи действия.

Мерките и действията относно кибер сигурността на производствените системи трябва да се планират дългосрочно, те трябва да са постоянни и адекватни на промените в технологиите и политико-географската обстановка, те трябва да се разглеждат многоаспектно предвид постоянно нарастващите хибридни заплахи за критичните инфраструктури, стратегически обекти и дейности от значение за националната сигурност.

Представени са рискови фактори, пропуски, уязвимости и няколко стъпки за конкретни действия в дългосрочен план за оценяване и отстраняване на риска от кибер инциденти и уязвимости в мрежите на ICS / SCADA. На база изложените стъпки могат да се изготвят адекватни план-мероприятия от организациите и фирмите, работещи с производствени системи.

СТЪПКИ:

Идентифициране на всички връзки към мрежите SCADA. Провеждане на задълбочен анализ на риска и оценяване на необходимостта от всяка връзка с мрежата SCADA. Разработване на цялостна схема за всички връзки към мрежата SCADA, колко добре са защитени те. Конкретизиране и оценяване на следните връзки:

- LAN и WAN, включително бизнес мрежите за организацията;
- Интернет;
- Безжични мрежови устройства, включително сателитни връзки;
- Модемни или комутируеми връзки;
- Връзки с бизнес партньори, доставчици, регулаторни агенции, трети страни.

Изключване на всички ненужни връзки към SCADA мрежите. За да се осигури най-висока степен на сигурност на системите SCADA, трябва същата да се изолира от другите мрежови връзки до възможно най-голяма степен. Всяка връзка с друга мрежа води до рискове за сигурността, особено ако връзката е от или към Интернет. Въпреки че директните връзки с други мрежови устройства могат да позволят обмяната на важна информация да бъде предавана ефикасно и удобно, несигурните връзки обикновено не си заслужават риска; *изолирането на мрежата SCADA трябва да бъде основна цел за осигуряване на необходимата защита*. Стратегии като използване на "демилитаризирани зони" (DMZ) и съхранение на данни биха могли да улеснят сигурното прехвърляне на данни от SCADA мрежата към бизнес мрежите. DMZ обаче трябва да бъдат проектирани и изпълнени правилно, за да се избегне внасянето на допълнителен риск от неправилно конфигуриране.

Оценяване и оптимизиране сигурността на всички останали връзки към SCADA мрежите. Мрежата SCADA е толкова сигурна, колкото и най-слабата й точка на свързване, важно е да се въведат защитни стени (Firewalls), системи за откриване на проникване (IDS) и други подходящи мерки за сигурност във всяка точка на влизане. Нужно е да се конфигурират правилата на защитната стена, за да се забрани достъпа от и до SCADA мрежата и да има възможно най-конкретни правила, когато се разрешават одобрени връзки.

Например независим системен оператор (ISO) не би трябвало да получава достъп до мрежата само защото има нужда от връзка с определени компоненти на SCADA системата. Стратегически трябва да се поставят IDS във всяка точка за влизане, за да може да се предупреждава персонала по сигурността за потенциални нарушения на сигурността на мрежата. Управлението на организацията трябва да разбира и да поема отговорност за рисковете, свързани с всяка връзка с мрежата SCADA.

Провеждане на тест за проникване и/или анализ на уязвимостта на всички останали връзки към мрежата SCADA, с цел да се оцени стойността на защитната стена (ако има такъв), свързана с тези пътища. Използване на тази информация във връзка с процесите за управление на риска, за да се разработи (предложи) стратегия за защита за всички пътища към SCADA мрежата.

Защита на SCADA мрежи чрез премахване или деактивиране на ненужните услуги. Пример за услуги, които могат да бъдат премахнати от мрежите на SCADA, включват автоматизирани системи за четене на данни/дистанционно отчитане, имейл услуги, достъп до Интернет.

Функция за деактивиране е също отдалечената поддръжка.

Трябва също да се работи в тясно сътрудничество с доставчиците на SCADA, за да бъдат идентифицирани сигурни конфигурации и да се съгласуват всички промени в операционните системи, за да е адекватно премахването или деактивирането на услуги, в резултат на което няма да се стигне до прекъсване на основната услугата или загуба на поддръжка.

Изпълнение на функциите за защита, предоставени от производителите на устройства и системи. Повечето по-стари SCADA системи (повечето системи в употреба) нямат никакви защитни елементи. Собствениците на системата SCADA трябва да настояват техният системен оператор да въвежда характеристики за сигурност под формата на корекции или подобрения на продукта. Някои по-нови SCADA устройства се доставят с основни защитни функции, но те обикновено са забранени, за да се осигури лесна инсталация.

Трябва да се анализира всяко SCADA устройство, за да се определите дали са налице защитните елементи. Освен това фабричните настройки по подразбиране за сигурност (например в защитните стени на компютърните мрежи) често са настроени така, че да осигуряват максимална използваемост, но минимална сигурност. Да се зададат всички функции за сигурност, за да се осигурите максимално ниво на сигурност. Да се позволят настройките за максимална сигурност само след задълбочена оценка на риска от последствията от намаляването на нивото на защита.

Да не се разчита на собствени протоколи за защита на системите. Някои SCADA системи използват уникални, патентовани протоколи за комуникация между полеви устройства и сървъри. Често сигурността на системите SCADA се основава единствено на тайната на тези протоколи. За съжаление, неяснотата по отношение на протоколите осигуряват много малко "реална" сигурност. Да не се разчита изцяло на собствените протоколи или на фабричните настройки по подразбиране за защита, за да се защитава системата. Трябва да се изиска от продавачите (доставчиците) да разкрият каквито и да е задни вратички или интерфейси на SCADA системите оставени за гаранционно и следгаранционно обслужване и да се очаква от тях да предоставят системи, които могат да бъдат защитени.

SCADA контролните сървъри, изградени върху различни търговски или отворени операционни системи, могат да бъдат изложени на атака и/или риск чрез стандартните мрежови услуги. В максимална степен, трябва да се премахнат или деактивират неизползваните услуги, за да бъде намален риска от директна атака. Това е с висока важност, когато мрежите SCADA са взаимосвързани с други мрежи (бизнес мрежи и/или други производствени високорискови мрежи).

Контрол върху всяка среда, която се използва като вратичка към мрежата SCADA. Когато в системите SCADA съществуват свързвания през „задна врата“ или доставчиците имат свързаност, трябва да се въведе усилено удостоверяване, за да бъдат сигурни комуникациите. Модемите, безжичните и кабелните мрежи, използвани за комуникации и поддръжка, представляват значителна уязвимост за мрежата SCADA. Успешните атаки “war dialing” или “war driving” могат да позволят на атакуващия да заобиколи всички други контроли и да има директен достъп до SCADA мрежата или ресурсите. За да се сведат до минимум рисковете от такива атаки, трябва да се деактивира входящия достъп и да се замени с някакъв тип система за обратно повикване.

Внедряване на системи за вътрешно и външно откриване на проникванията и създаване на 24-часово наблюдение на инцидентите. За да може ефективно да се реагира на кибернетичните атаки, трябва да се създаде стратегия за откриване на проникванията, която включва предупреждаване на мрежовите администратори за злонамерена мрежова активност, произхождаща от вътрешни или външни източници. Проследяването на

системата за откриване на проникванията е от съществено значение 24 часа в денонощието; тази възможност може лесно да се настрои и чрез системи за мрежово сканиране и/или защитни стени. Трябва да има процедури за реагиране при инциденти, които да позволяват ефективен отговор на всяка атака. За да се осъществи мониторинг на мрежата, да се активира ежедневното регистриране на всички системи и дневници на системата за одит, за да може да се открива подозрителната активност възможно най-скоро.

Извършване на технически одити на SCADA устройства и мрежи и всякакви други свързани мрежи, за да се идентифицират проблеми, свързани със сигурността. Техническите одити на SCADA устройства и мрежи са от решаващо значение за продължаващата ефективност на сигурността. Има много инструменти за сигурност с търговска цел и с отворен код, които позволяват на системните администратори да извършват одити на своите системи и мрежи, за да се идентифицират активните услуги, нивото на кръпки (Patches) и често срещаните уязвимости. Използването на тези инструменти не разрешава системни проблеми, а премахва "пътищата на най-малка съпротива", които един кибер нападател може да използва. Да се анализират установените уязвимости, за да се определи тяхното значение и след това да се предприемат коригиращи действия. Да се проследяват коригиращите действия и да се извършва анализ на тази информация, за да се установят тенденциите. В допълнение, повторното тестване след коригиращите действия, ще гарантира, че уязвимите места всъщност са елиминирани. Да се сканират непроизводствените среди активно, за да се откриват и отстраняват потенциални проблеми.

Провеждане на проучвания за физическа сигурност и оценяване на всички отдалечени обекти, свързани с мрежата SCADA, за да се оцени тяхната сигурност. Всяко местоположение, което има връзка с мрежата SCADA, е цел, особено неконтролирани и/или не охранявани отдалечени сайтове. Да се провеждат проучване за физическа сигурност и точки за достъп до инвентара във всяко съоръжение, което има връзка със системата SCADA. Да се идентифицират и оценят всеки източник на информация, включително дистанционна телефонна / компютърна мрежа / оптични кабели, които могат да бъдат подслушвани; радио и микровълнови връзки, които могат да бъдат експлоатирани; компютърни терминали, които могат да бъдат достъпни; безжични точки за достъп до локалната мрежа. Да се идентифицират и елиминират единичните точки на отказ. Сигурността на сайта трябва да е достатъчна за откриване или предотвратяване на неоторизиран достъп. Да не се допускат "живи" точки за достъп до мрежата на отдалечени, не охранявани места просто за удобство.

Създаване на SCADA Екипи за идентифициране и оценка на възможни сценарии за атака. Да се създаде SCADA Екип, за да се идентифицират потенциалните сценарии за атака и да се преценят потенциалните уязвимости на системата. Да се използват различни хора/група от хора, които могат да дадат представа за слабостите на цялата мрежа, SCADA системите, физическите системи и контролите за сигурност. Хората, които работят със системата всеки ден, имат ясна представа за уязвимостта на SCADA мрежата и трябва да бъдат консултирани при идентифицирането на потенциални сценарии за атака и възможни последици. Също така, трябва да се провери, че рискът от злонамерен вътрешен човек е напълно и правилно оценен, тъй като това представлява една от най-големите заплахи за дадена организация. След предоставяне на информация от SCADA Екип за процесите за управление на риска, да се оцени информацията и да се установят подходящи стратегии за защита.

Да се определят ясно ролите, отговорностите и отговорностите на кибер сигурността за мениджърите, системните администратори и потребителите. Създаване на организационна структура за кибер сигурност (ИБ/ИС/КС), която да определя ролите и отговорностите и ясно да определя как се ескалират (насочват) проблемите на кибер сигурността, кой е уведомен в извънредна ситуация.

Персоналът в организацията трябва да разбере специфичните очаквания, свързани със защитата на ресурсите на информационните технологии чрез дефинирането на ясни и логически роли, правила и отговорности. Освен това, ключовият персонал трябва да има достатъчно правомощия да изпълнява възложените му отговорности. Твърде често "добрата" кибер сигурност се оставя на инициативата на индивида, което обикновено води до непоследователни внедрявания и неефективна сигурност.

Документиране на мрежовата архитектура и идентифициране на системи, които обслужват критични функции или съдържат чувствителна информация, която изисква допълнителни нива на защита. Разработване и документиране на стабилна архитектура за сигурност на информацията като част от процес за създаване на ефективна стратегия за защита. От съществено значение е организацията да проектира своите мрежи с оглед на сигурността и да продължава да има ясно разбиране за мрежовата си архитектура през целия си жизнен цикъл. От особено значение е задълбоченото разбиране на функциите, които системите изпълняват и чувствителността на съхраняваната информация. Без това разбиране рискът не може да бъде правилно оценен и стратегиите за защита може да не бъдат достатъчни. Документирането на архитектурата за сигурност на информацията и нейните компоненти е от решаващо значение за разбирането на цялостната стратегия за защита и идентифицирането на единични точки на отказ („single points of failure“).

Установяване на строг, текущ процес на управление на риска. Пълното разбиране на рисковете за мрежовите компютърни ресурси от атаките „Отказ на услуга“ и уязвимостта на чувствителната информация до компромис е от съществено значение за ефективността на програмата за кибер сигурност. Оценките на риска представляват техническата база на това разбиране и са от решаващо значение за формулирането на ефективни стратегии за смекчаване на уязвимостите и запазване на целостта на компютърните ресурси. Първоначално трябва да се извърши основен анализ на риска въз основа на текуща оценка на заплахите, която да използвате за разработването на стратегия за защита на мрежата. Поради бързо променящата се технология и появата на нови заплахи на дневна база е необходим и постоянен процес за оценка на риска, за да могат да се направят рутинни промени в стратегията за защита, за да се гарантира, че тя остава ефективна. Основното за управлението на риска е идентифицирането на остатъчния риск със стратегия за защита на мрежата и приемането на този риск от ръководството.

Създаване на стратегия за защита на мрежата, основаваща се на принципа на задълбочена защита. Основен принцип, който трябва да бъде част от всяка стратегия за защита на мрежата, е защитата в дълбочина. Задачата на защитата трябва да бъде разгледана в началото на етапа на разработване и трябва да бъде неразделна част от всички технически решения, свързани с мрежата. Да се използват технически и административни контроли, за да се смекчат заплахите от установени рискове до възможно най-голяма степен на всички нива в мрежата. Единичните точките на неуспех „Single points of failure“ трябва да се избягват и защитата на кибер сигурността трябва да бъде така наслоена, че да ограничи въздействието на всеки инцидент по сигурността. Всеки слой трябва да бъде защитен срещу

други системи на същия слой. Например, за да се предпазим от вътрешната заплаха, трябва да ограничим потребителите да имат достъп само до онези ресурси, необходими за изпълнение на техните функции.

Ясно да се определят изискванията за кибер сигурност. Необходими са структурирани програми за сигурност, които поставят задължителни изисквания, за да се създадат очаквания и да се позволи на служителите да бъдат държани отговорни. Официалните политики и процедури обикновено се използват за създаване и институционализиране на програма за кибернетична сигурност. Официалната програма е от съществено значение за установяването на последователен, базиран на стандарти подход към кибернетичната сигурност в цялата организация и елиминира единствената зависимост от нежелана инициатива. Политиките и процедурите също така информират служителите за техните специфични отговорности в областта на кибернетичната сигурност и последствията от неспазването на тези отговорности. Те предоставят насоки относно действията, които трябва да се предприемат по време на инцидент с кибернетична сигурност и насърчават ефикасни и ефективни действия по време на криза. Като част от определянето на изискванията за кибернетична сигурност, да включват потребителски споразумения и уведомяващи и предупредителни банери. Създаване на изисквания за свеждане до минимум на заплахата от злонамерени вътрешни лица, включително необходимостта от извършване на проверки на място и ограничаване на мрежовите привилегии до тези, които са абсолютно необходими.

Създаване и спазване на ефективни процеси/действия за управление на конфигурацията. Основният процес на управление, необходим за поддържането на сигурна мрежа, е *управлението на конфигурацията*. Управлението на конфигурацията трябва да *обхваща както хардуерните конфигурации, така и софтуерните конфигурации*. Промените в хардуера или софтуера могат лесно да въведат уязвимости, които подкопават сигурността на мрежата. Необходими са процеси за оценка и контрол на всяка промяна, за да се гарантира, че мрежата остава сигурна. Управлението на конфигурацията трябва да започва с добре проверени и документирани базови линии за сигурност за различните системи.

Провеждане на рутинни самооценки. Необходими са ясни процеси за оценка на ефективността, за да се предостави на управлението обратна връзка относно ефективността на политиката в областта на кибер сигурността и техническото изпълнение. Признак на зрялост на организацията е възможността да се идентифицират проблемите, да се извърши анализ на коренните причини и да се приложат ефективни коригиращи действия, насочени към индивидуални и системни проблеми. Процесите на самооценка, които обикновено са част от ефективна програма за кибер сигурност, включват рутинно сканиране за уязвимости, автоматизирано одитиране на мрежата и самооценка на организационните и индивидуалните резултати.

Създаване на резервни копия на системата и планове за възстановяване след бедствие и/или атаки. Да се създаде план за възстановяване след бедствие, който позволява бързо възстановяване от всякакви аварийни ситуации (включително кибер атаки). Системните архиви са съществена част от всеки план и позволяват бърза реконструкция на мрежата. Рутинно да се изпълняват планове за възстановяване при бедствия, за да се гарантира, че те работят и че персоналът е запознат с тях. Да се направят подходящи

промени в плановете за възстановяване след бедствие въз основа на извлечените поуки от упражненията.

Висшето ръководство на организацията трябва да създава очаквания за изпълнение на кибернетичната сигурност и да държи хората отговорни за изпълнението им. Ефективната кибер сигурност изисква ангажираност и лидерство от висши мениджъри в организацията. От съществено значение е висшето ръководство да създаде очакване за силна кибернетична сигурност и да съобщи това на своите подчинени мениджъри в цялата организация. Също така е от съществено значение висшето организационно ръководство да създаде структура за изпълнение на програма за кибернетична сигурност. Тази структура ще насърчи последователното изпълнение и способността да поддържат силна програма за кибернетична сигурност. Важно е хората да бъдат държани отговорни за изпълнението им, тъй като се отнася до кибернетичната сигурност. Това включва мениджъри, администратори на системи, техници и потребители, оператори.

Документиране. Изготвяне на политики и провеждане на обучение, за да се сведе до минимум вероятността персонала в организацията по невнимание да разкрие чувствителна информация относно дизайна на системата SCADA, операциите или контрола за сигурност. "Социалното инженерство", събирането на информация за компютри или компютърна мрежа чрез въпроси към наивни потребители, често е първата стъпка в злонамерената атака срещу компютърните мрежи. Колкото повече информация се разкрива за компютрите или компютърната мрежа, толкова по-уязвима става тя. Никога не трябва да се разгласяват данни, свързани със SCADA мрежата, включително имената и информацията за контактите относно системните оператори / администратори, компютърните операционни системи и / или физическото и логическото локализиране на компютри и мрежови системи по телефони или на персонал, освен ако не са изрично упълномощени да получават такава информация. Всяко искане за информация от неизвестни лица трябва да бъде изпратено до централно място за сигурност за проверка и изпълнение. **Хората могат да бъдат слаба връзка в иначе сигурна мрежа.** Да се провеждат обучения и информиране, за да се гарантира, че персоналът остава усърден при защитата на чувствителна мрежова информация, особено на паролите си. Разпространяване на данни, свързани с мрежата SCADA се предоставят само на стриктно основание и при необходимост да се знае, и само на лица, изрично упълномощени да получават такава информация.

Следва ...