Доклад

Киберсигурност в групата Енерго-Про

В края на месец юни 2012 г. ЕНЕРГО-ПРО закупи бизнеса на немската компания Е.ОН в България и по този начин придоби компании, притежаващи лицензии за следните дейности в енергетиката:

- разпределение на електрическа енергия (Електроразпределение Север АД);
- снабдяване с електрическа енергия (ЕНЕРГО-ПРО Продажби АД);
- търговия с електрическа енергия и координатор на стандартна балансираща група (ЕНЕРГО-ПРО Енергийни Услуги ЕООД).

Лицензионната територия е с размер от близо 30 000 кв.км и покрива 9 административни области в Североизточна България - Варна, Велико Търново, Габрово, Добрич, Разград, Русе, Силистра, Търговище и Шумен. За доброто обслужване на клиентите са обособени 13 центъра за обслужване на клиенти, разположени в 11 града в Североизточна България и денонощен телефонен център.

Сама по себе си дейността на един екип по киберсигурност се подчинява на правилото „Не можем да се борим срещу нещо, което не разбираме“. По тази причина мисията ни е да правим и двете, а именно да защитаваме, постоянно учейки, и да се борим, постоянно информирайки.

От тази гледна точка в Енерго-Про беше създадена работна група по киберсигурност с основна цел да съдейства за защитата на информационните ресурси на компанията, както и да обучава колегите си по отношение на безопасното използване на тези ресурси.

Беше създадена и СУИС – система за управление на информационната сигурност.

Тя гарантира подбор на адекватни и пропорционални контроли за информационна сигурност и поддръжка на механизми за обмен на информация, които позволяват информирани решения и своевременни действия.

Целите, политиките и процедурите на компанията са съобразени с бизнес целите на компанията и очакванията на заинтересованите страни. Отговорен за управлението и поддържането на СУИС е представител на УС. Мениджърите са пряко отговорни за прилагането на тази политика и за гарантиране на съответствие на персонала в техните области на отговорност. Работната група по сигурността, начело с Главен изпълнителен директор е основният орган за информационна сигурност.

СУИС се отнася за информацията и информационните системи, управлявани от компанията в нашите офиси, разположени в 11-те града на Североизточна България. Не се допускат изключения от изискванията на ISO 27001:2017 и Закона за киберсигурност на Република България.

Целта на политиката за информационна сигурност е да се сведат до минимум бизнес рисковете, да се максимизират бизнес възможностите и да се запази спазването на законодателните, регулаторните и договорните изисквания.

Политиката включва:

- защита на поверителността, целостта и достъпността на информацията;

- защита на чувствителна информация от неоторизиран достъп или използване;
- гарантиране, че нарушенията на сигурността и инцидентите се докладват навреме и се разследват;
- гарантиране, че нарушенията в политиката за информационна сигурност се управляват;
- непрекъснато оценяване на бизнес дейностите за премахване или смекчаване на заплахите;
- гарантиране, че целият персонал е обучен по отношение на информационната сигурност и информираност;
- гарантиране, че достъпът на външни лица до информацията се контролира;
- поддържане на планове за непрекъснатост на дейността по отношение на критичните дейности в бизнеса, както и за възстановяване при бедствия и аварии;
- спазване на законодателните, регулаторните и договорните изисквания;
- непрекъснато подобряване на системата за управление на информационната сигурност.

Политиките и процедурите, заложени в СУИС надхвърлят изискванията на Закона за киберсигурност на Р България и се придържат плътно към изискванията, заложени в ISO 27001 и PCI DSS. От месец юни 2020 компанията притежава сертификат по ISO 27001 за „*Защита на всички видове информация, обработвана във връзка с предоставяне на IT услуги към дружествата от групата на Енерго-Про. Система за управление на информационната сигурност, приложена при проектиране, разработка и внедряване на хардуер и софтуер в областта на Енергетиката и бизнеса*“.

Информационната сигурност има два аспекта – физически и логически (електронен). СУИС на Енерго-Про обхваща и двата аспекта.

Физическа сигурност на информацията

По отношение на този аспект са въведени в експлоатация редица мерки и правила, гарантиращи физическото опазване на информацията, както и контрола до нея. Какво включва това?

1. Контрол на достъпа до сградите, в които се съхранява или обработва важната за компанията информация. В тази връзка компанията разполага с денонощна физическа охрана, организирана в съответствие с изискванията на законите на Р България и поставените задачи от страна на УС.
2. Денонощно видеонаблюдение на всички важни за компанията съоръжения, сгради, етажи и помещения. Съхранение на записи за бъдещи разследвания.
3. Договор с външен доставчик на услугата СОТ, разполагащ със записи на всички събития за евентуално използване при вътрешни разследвания.
4. Контрол на достъпа с безконтактни карти, като са обособени няколко зони на достъп в зависимост от важността им за компанията. Записи за няколко месеца назад, гарантиращи проследяването на даден служител в случай на разследване.
5. Изграждане и поддръжка на пожароизвестяваща и пожарогасяща система. Записи на събитията, свързани с тази система.
6. Изгради се център за възстановяване при бедствия и аварии, който би послужил при проблем с основния колокационен център на компанията.

7. Въведени са и са сведени до всички служители правила за ползване на работните места, като например „чисто бюро и чист екран“.

8. Всички преминаха цикъл от материали за обучение по киберсигурност на всички служители в компанията, които не са специалисти в ИТ.

9. Отделя се специално внимание на физическото съхранение и сигурното унищожаване на физически носители на информация, която е чувствителна за компанията.

10. Редовни вътрешни одити по отношение на гореизброените мерки за физическа сигурност.

11. Всеки новопостъпил служител преминава през начално обучение по СУИС в зависимост от позицията, на която е назначен.

Електронна (логическа) сигурност

Дейността на компанията, която е от национално значение, е разпространението на електрическа енергия. В тази връзка, както и във връзка с Наредбата на ДАНС, УС на Енерго-Про определи, като такава системата SCADA за диспечеризиране на разпространението на ел.енергия. Въведени са редица мерки за защита на тази система по отношение на нейната непрекъсваемост и защита от нерегламентирано посегателство.

Като част от мерките мога да спомена:

1. Недостъпност от Интернет. Системата работи в своя собствена мрежа без достъп от/до Интернет.

2. Сървърите на системата са разположени в няколко града и са взаимно допълващи се (двупосочен миръринг). Разположени са в специални помещения, изградени в съответствие с изискванията на световните добри практики.

3. Всички диспечерски станции (компютри) са снабдени с антивирусна защита.

4. Достъпът до сървърите е строго филтриран на физическо и електронно ниво.

5. Периодично се извършва вътрешен одит на системата от страна на дирекцията по вътрешен одит по отношение, както на физическата, така и на логическата защита на системата.

6. Мрежата, през която се осъществява комуникацията, е базирана на VPN технологията.

По отношение на останалите дейности на компанията, мерките, въведени в експлоатация във връзка със защитата на информацията, са стандартни, т.е. се подчиняват на изискванията в най-силните стандарти за информационна сигурност. Като такива мога да спомена:

1. Наличие на независими локални мрежи в зависимост от предназначението им. Филтриране на ниво защитни стени.

2. Прилагане на строга e-mail защита по отношение на получаването или разпространението на зловредна кореспонденция.

3. Наблюдение на трафика чрез използването на WAF (Web Application Firewall).

4. Антивирусна защита на всички работни станции.

5. Използване на активна директория за достъп до всички компютърни системи. Строги правила за работа, включващи: периодична промяна на потребителската парола

(изисквания за сложност и неповторяемост), заключване на екрана след няколко минутно неизползване на компютъра, забрана за инсталиране на приложения и др.

6. Отдалечен достъп до корпоративната мрежа само през защитен със сертификат тунел (VPN).

7. Строги правила за сигурно програмиране в унисон с изискванията на Open Web Application Security Project (OWASP). Това включва и всички наши външни изпълнители на проекти по отношение на програмирането.

8. Договори с доставчици за навременна защита от DDoS атаки. Тази мярка включва ограничаване на достъпа до сървърите ни само в рамките на България или туширане на атаката още в рамките на страните, откъдето е започнала.

9. Изисквания за конфиденциалност на информацията, редовни проверки за наличие на „слушатели“ (man-in-the-middle) по мрежата на доставчика, както и на своевременна реакция при откриване на аномалии, свързани с доставката на услугата.

10. Изградихме лаборатория по киберсигурност, в която могат да се наподобят различни атаки, да се изследват съмнителни писма в сигурна среда да се обучават колеги по отношение на безопасното използване на Интернет.

11. Периодични вътрешни одити на ключови за компанията мрежи и сървъри за наличието на уязвимости.

12. Периодично обучение на всички служители от групата Енерго-Про по отношение на киберсигурността.

13. Покрихме изискванията на ISO 27001 и от юни месец 2020 притежаваме сертификат по стандарта. В тази връзка осъществяваме периодични вътрешни одити по СУИС във всички 11 града на територията на компанията.

В заключение мога да кажа, че ръководството на Енерго-Про се отнася изключително сериозно към въпросите, свързани със сигурността на информацията и полага ежедневни усилия за преодоляване на проблемите, свързани с този аспект.

Автор: Станислав Чакъров

Специалист по корпоративна сигурност

Енерго-Про Варна