IXPERTA

AKO VYBUDOVAŤ DIGITÁLNU PEVNOSŤ

Andrej Kavický
29.3.2023
www.ixperta.com

Prečo potrebujeme smernicu

Kyberpriestor ako jedno spoločné prostredie
- potreba jasných pravidel pre každého

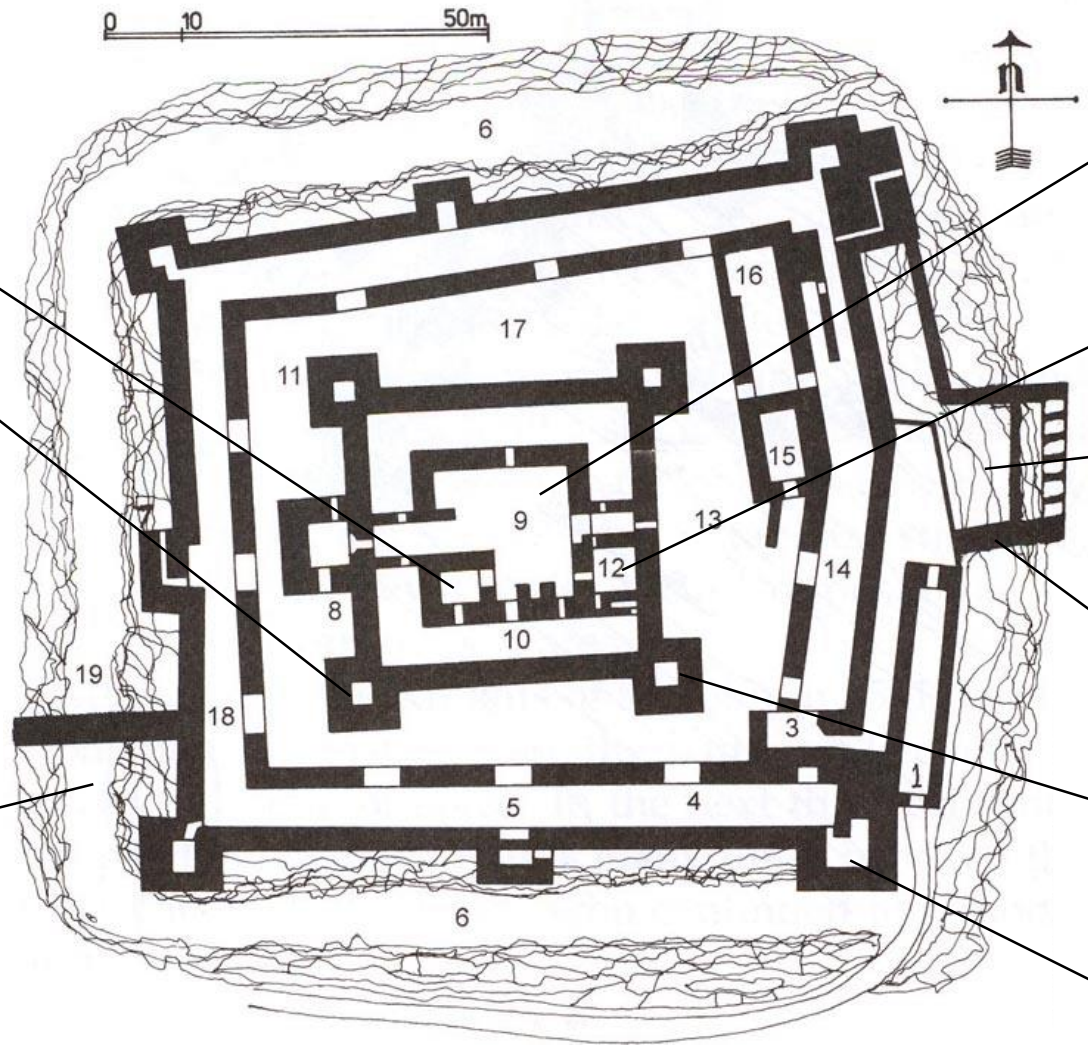
Najslabší článok
- útočník hľadá najslabšie miesto

NIS2 dáva predpoklad pre dobrý základ pre bezpečné prostredie
- dobrá príležitosť vybudovať si silnú ochranu

Technológie nie sú všetko
- bezpečnosť je hlavne o ľuďoch

IXPERTA

Ako sa poučiť z histórie?



Archív

Datacenter Firewall

Endpoint Protection

Data Loss Prevention

Dáta

Backup

Dvojfaktorová autentifikácia

Perimeter Next-Gen Firewall

Log Management/SIEM/SOC

Intrusion Detection/Prevention System

IXPERTA

Základné opatrenia podľa NIS 2

- ✓ Zásady analýzy rizík a bezpečnosti informačných systémov
- ✓ Riešenie incidentov
- ✓ Kontinuita činností – riadenie zálohovania, obnova systému
- ✓ Bezpečnosť dodávateľského reťazca
- ✓ Bezpečnosť siete a informačných systémov vrátane riešenia zraniteľností
- ✓ Zásady postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík
- ✓ Základné postupy kybernetickej hygieny
- ✓ Zásady a postupy používania kryptografie a
- ✓ Bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správa aktív
- ✓ Používanie viacstupňovej autentifikácie

Základné opatrenia podľa NIS 2

Protiopatrenia v oblasti kybernetickej bezpečnosti sú technické (technológie) a organizačné (procesy a dokumentácia)

NIS 2 bude aplikovaný do Zákona o KB

Základné opatrenia podľa NIS 2

- ✓ Zásady analýzy rizík a bezpečnosti informačných systémov
- ✓ Riešenie incidentov
- ✓ Kontinuita činností – riadenie zálohovania, obnova systému
- ✓ Bezpečnosť dodávateľského reťazca
- ✓ Bezpečnosť siete a informačných systémov vrátane riešenia zraniteľností
- ✓ Zásady postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík
- ✓ Základné postupy kybernetickej hygieny
- ✓ Zásady a postupy používania kryptografie a
- ✓ Bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správa aktív
- ✓ Používanie viacstupňovej autentifikácie

Firemné zlato

Opatrenie NIS 2: Zásady analýzy rizík a bezpečnosti informačných systémov

Čo potrebujeme skutočne chrániť?

Čo nám hrozí?

Aké opatrenia už som urobil?

Analýza rizík

Interný audit/externý audit

Návrh a prioritizácia opatrení

IXPERTA

Základné opatrenia podľa NIS 2

- ✓ Zásady analýzy rizík a bezpečnosti informačných systémov
- ✓ Riešenie incidentov
- ✓ Kontinuita činností – riadenie zálohovania, obnova systému
- ✓ Bezpečnosť dodávateľského reťazca
- ✓ Bezpečnosť siete a informačných systémov vrátane riešenia zraniteľností
- ✓ Zásady postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík
- ✓ Základné postupy kybernetickej hygieny
- ✓ Zásady a postupy používania kryptografie a
- ✓ Bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správa aktív
- ✓ Používanie viacstupňovej autentifikácie

Ako pripraviť tím

Opatrenie NIS 2: Riešenie incidentov

Viem o incidentoch v mojich IS?

Ako môj tím reaguje na incident?

Mám vybudovaný proces riadenia incidentov?

Zavedenie manažmentu incidentov

Detekcia incidentov – technologické opatrenie

Klasifikácia incidentov

IXPERTA

Základné opatrenia podľa NIS 2

- ✓ Zásady analýzy rizík a bezpečnosti informačných systémov
- ✓ Riešenie incidentov
- ✓ Kontinuita činností – riadenie zálohovania, obnova systému
- ✓ Bezpečnosť dodávateľského reťazca
- ✓ Bezpečnosť siete a informačných systémov vrátane riešenia zraniteľností
- ✓ Zásady postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík
- ✓ Základné postupy kybernetickej hygieny
- ✓ Zásady a postupy používania kryptografie a
- ✓ Bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správa aktív
- ✓ Používanie viacstupňovej autentifikácie

IXPERTA

Prišiel som o dáta

Opatrenie NIS 2: Kontinuita činností – riadenie zálohovania, obnova systému

Mám pripravené plány?

Čo potrebujem zálohovať?

Ako rýchlo potrebujem obnoviť svoju IS?

Definícia požiadaviek

Nemeniteľná záloha

Dátová a aplikačná konzistencia

IXPERTA

Základné opatrenia podľa NIS 2

- ✓ Zásady analýzy rizík a bezpečnosti informačných systémov
- ✓ Riešenie incidentov
- ✓ Kontinuita činností – riadenie zálohovania, obnova systému
- ✓ Bezpečnosť dodávateľského reťazca
- ✓ Bezpečnosť siete a informačných systémov vrátane riešenia zraniteľností
- ✓ Zásady postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík
- ✓ Základné postupy kybernetickej hygieny
- ✓ Zásady a postupy používania kryptografie
- ✓ Bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správa aktív
- ✓ Používanie viacstupňovej autentifikácie

IXPERTA

Spoznaj svojho obchodného partnera

Opatrenie NIS 2: Bezpečnosť dodávateľského reťazca

Čo viem o svojich obchodných partneroch?

Môžu pristupovať k mojim dátam?

Čo robia v mojej sieti?

Zavedenie procesov pre kontrolu dodávateľov

Zavedenie správy privilegovaných účtov

Bezpečné externé pripojenie

IXPERTA

Základné opatrenia podľa NIS 2

- ✓ Zásady analýzy rizík a bezpečnosti informačných systémov
- ✓ Riešenie incidentov
- ✓ Kontinuita činností – riadenie zálohovania, obnova systému
- ✓ Bezpečnosť dodávateľského reťazca
- ✓ Bezpečnosť siete a informačných systémov vrátane riešenia zraniteľností
- ✓ Zásady postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík
- ✓ Základné postupy kybernetickej hygieny
- ✓ Zásady a postupy používania kryptografie
- ✓ Bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správa aktív
- ✓ Používanie viacstupňovej autentifikácie

IXPERTA

„Bratříčku zavírej vrátka“

Opatrenie NIS 2: Bezpečnosť siete a informačných systémov vrátane riešenia zraniteľností

Kedy sa mám venovať bezpečnosti?

Ako bezpečné je moje prostredie?

Trvalé posudzovanie bezpečnosti systémov

Kontinuálna kontrola zraniteľností

Odstraňovanie zraniteľností

IXPERTA

Základné opatrenia podľa NIS 2

- ✓ Zásady analýzy rizík a bezpečnosti informačných systémov
- ✓ Riešenie incidentov
- ✓ Kontinuita činností – riadenie zálohovania, obnova systému
- ✓ Bezpečnosť dodávateľského reťazca
- ✓ Bezpečnosť siete a informačných systémov vrátane riešenia zraniteľností
- ✓ Zásady postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík
- ✓ Základné postupy kybernetickej hygieny
- ✓ Zásady a postupy používania kryptografie
- ✓ Bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správa aktív
- ✓ Používanie viacstupňovej autentifikácie

Bezpečnosť ako dobre fungujúci stroj

Opatrenie NIS 2: Zásady a postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík
Základné postupy kybernetickej hygieny

Ako si overím nastavené pravidlá?

Aká je miera znalostí užívateľov?

Čo robia zamestnanci v prostredí firemnej IS?

GAP analýza a audit

Vzdelávanie zamestnancov v oblasti KB, overovanie znalostí

Zavedenie DLP

IXPERTA

Základné opatrenia podľa NIS 2

- ✓ Zásady analýzy rizík a bezpečnosti informačných systémov
- ✓ Riešenie incidentov
- ✓ Kontinuita činností – riadenie zálohovania, obnova systému
- ✓ Bezpečnosť dodávateľského reťazca
- ✓ Bezpečnosť siete a informačných systémov vrátane riešenia zraniteľností
- ✓ Zásady postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík
- ✓ Základné postupy kybernetickej hygieny
- ✓ Zásady a postupy používania kryptografie
- ✓ Bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správa aktív
- ✓ Používanie viacstupňovej autentifikácie

IXPERTA

Posilnená ochrana

Opatrenie NIS 2: Zásady a postupy používania kryptografie
Bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správa aktív
Používanie viacstupňovej autentifikácie

Ako chrániť dáta?

Kto sa prihlasuje do mojej siete?

Prečo mi nestačí antivírus?

Šifrovanie komunikácie a dát

Implementácia overovania identity

Ochrana koncových staníc EDR/XDR

IXPERTA

Sumár

Priority

Riziká

Ľudia

IXPERTA

IXPERTA

ĎAKUJEM ZA POZORNOSŤ

Andrej Kavický
andrej.kavicky@ixperta.com