Valstybinės augalininkystės tarnybos prie Žemės ūkio ministerijos informacinės sistemos veiklos tęstinumo valdymo plano
6 priedas

KRITERIJŲ, KURIAIS VADOVAUJANTIS ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTAI PRISKIRIAMI ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ KATEGORIJOMS, SĄRAŠAS

Eil. Nr.	**Elektroninės informacijos saugos incidento grupės**	**Elektroninės informacijos saugos incidento poveikis** / **Elektroninės informacijos saugos incidento pogrupiai**	**Nereikšmingas (N)** (bent vienas iš kriterijų)				**Vidutinis (V)** (du ar daugiau kriterijų)					**Didelis (D)** (du ar daugiau kriterijų)				**Pavojingas (P)** (bent vienas iš kriterijų)			
			VATIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	VATIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar VATIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	VATIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar VATIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	VATIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše
1.	Nepageidaujamų laiškų, klaidinančios ar žeidžiančios informacijos platinimas (angl. *abusive content*, *spam*)	1.1. Nepageidaujami laiškai ir (ar) klaidinančios, žeidžiančios informacijos platinimas trikdo Valstybinės augalininkystės tarnybos prie Žemės ūkio ministerijos informacinės	N				V					D				P			

		sistemos (toliau – VATIS)) veiklą ir (ar) teikiamas paslaugas				
		1.2. Nepageidaujamų laiškų ir (ar) klaidinančios, žeidžiančios informacijos platinimas	N			
2.	Kenkimo programinė įranga (angl. *malicious software / code*) Programinė įranga ar jos dalis, kuri padeda neteisėtai prisijungti prie VATIS, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jų veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę ja naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims	2.1. Aptikta moderni kenkimo programinė įranga (angl. *advanced persistent threat, APT*)		V	D	P
		2.2. VATIS aktyviai kontroliuojama įsibrovėlių (pavyzdžiui, „galinės durys“ (angl. *back door*), kompiuterizuotos darbo vietos ar tarnybinės stotys tampa „Botinklo“ (angl. *Botnet*) infrastruktūros dalimi		V	D	P
		2.3. Kenkimo programinė įranga, trikdanti saugumo priemonių darbą		V	D	P
		2.4. Kenkimo programinė įranga, kurią aptinka saugumo priemonės per reguliarų patikrinimą ir (ar) kurią saugumo priemonės automatiškai blokuoja	N	V		
		2.5. Kenkimo programinė įranga, platinama naudojant socialinės inžinerijos metodus	N	V	D	P
3.	Informacijos rinkimas (angl. *information gathering*) Žvalgyba ar kita įtartina veikla (angl. *scanning, sniffing*), manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl. *social engineering*), siekiant stebėti ir rinkti informaciją, atrasti silpnąsias vietas, atlikti grėsmę keliančius veiksmus, apgavystės, siekiant įtikinti naudotoją atskleisti informaciją (angl. *phishing*) arba atlikti norimus veiksmus	3.1. VATIS paketų / informacijos perėmimas		V	D	P
		3.2. VATIS klastojimas, siekiant surinkti prisijungimo ar kitą svarbią informaciją, tiksliniai laiškai, kuriuose, pasinaudojant socialinės inžinerijos principais, siekiama išvilioti prisijungimo ir (ar) kitą svarbią informaciją, priversti atlikti norimus veiksmus (pvz., finansines operacijas)		V	D	P
		3.3. Vykdoma perimetro priemonių žvalgyba (nebandant įsilaužti)	N	V		
		3.4. Naudojami socialinės inžinerijos metodai, siekiant išvilioti prisijungimo prie VATIS ir (ar) kitą svarbią informaciją	N	V		
4.	Mėginimas įsilaužti (angl. *intrusion attempts*)	4.1. Išnaudojamas vienas ar keli nežinomi (angl. *zero day*) pažeidžiamumai, siekiant		V	D	P

	Mėginimas įsilaužti arba sutrikdyti VATIS veikimą išnaudojant žinomus pažeidžiamumus (angl. *exploiting of known vulnerabilities*), bandant parinkti slaptažodžius (angl. *login attempts*), kitą įsilaužimo būdą (angl. *new attack signature*)	tikslingai sutrikdyti konkrečią VATIS dalį				
		4.2. Išnaudojamas vienas ar keli nežinomi (angl. *zero day*) pažeidžiamumai	N	V	D	P
		4.3. Vidinė VATIS žvalgyba ar kita kenkimo veika (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita)		V	D	P
		4.4. Išnaudojami žinomi ir viešai publikuoti pažeidžiamumai arba atliekami bandymai prisiijungti prie VATIS parenkant slaptažodžius	N	V		
5.	Įsilaužimas (angl. *intrusions*) Sėkmingas įsilaužimas ir (ar) neteisėtas VATIS, taikomosios programinės įrangos ar paslaugos naudojimas (angl. *privileged account compromise, unprivileged account compromise, application compromise*)	5.1. Veiksmai prieš VATIS ar jos saugumo priemones, informacijos pasisavinimas, naikinimas, VATIS ar jos dalies pažeidimas, sutrikdantis VATIS teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti VATIS naudotojų pasitikėjimą jais		V	D	P
		5.2. Gaunama neteisėta prieiga prie VATIS, taikomosios programinės įrangos ar paslaugos		V	D	P
6.	Paslaugų trikdymas, prieinamumo pažeidimai (angl. *availability*) Veiksmai, kuriais trikdoma VATIS veikla, teikiamos paslaugos (angl. *DoS, DDoS*), VATIS ar jos dalies pažeidimas, sutrikdantis VATIS ir (ar) jos teikiamas paslaugas (angl. *sabotage, outage*)	6.1. Teikiamų paslaugų nutraukimas arba maksimalaus leistino paslaugos neveikimo laiko viršijimas		V	D	P
		6.2. Teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui	N	V		
		6.3. Aptinkamas paslaugos trikdymas, kuris neturi įtakos paslaugų teikimui	N	V		
7.	Informacijos turinio saugumo pažeidimai (angl. *information content security*) Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas (angl. *unauthorised access to*	7.1. Neteisėta prieiga prie informacijos, galinčios turėti įtakos VATIS veiklai ir (ar) teikiamoms paslaugoms		V	D	P
		7.2. Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas	N	V	D	P

	information, unauthorised modification of information)					
8.	Neteisėta veikla, sukčiavimas (angl. *fraud*) Vagystė, apgavystė, neteisėtas išteklių (angl. *unauthorized use of resources*), nelegalios programinės įrangos ar autorių teisių (angl. *copyright*) naudojimas, tapatybės klastojimo, apgavystės ir kiti panašaus pobūdžio incidentai	8.1. Neteisėta įtaka VATIS veiklai ir (ar) teikiamoms paslaugoms	N	V	D	P
9.	Kita Incidentai, kurie neatitinka nė vienos iš nurodytų grupių aprašymų		N	V	D	P