Hodnocení a postup při řešení bezpečnostního incidentu CSIRT týmem MASTER.CZ-CSIRT
V rámci response týmu je nutné zpracovávat, vyhodnocovat a evidovat jednotlivé typy incidentů.

Úroveň rizika
V následující tabulce jsou popsány úrovně rizika, které identifikujeme.

Úroveň rizika	Definice rizika	Typický incident	Typický následek incidentu	Response time
3	Vysoké	DoS	Nedostupnost, ohrožení integrity aktiv	60 minut
2	Střední	Scanning	Ohrožení aktiva	24 hodin
1	Nízké	Spam	Stížnost, oznámení	Další pracovní den

Identifikace
Tímto krokem je nutné ověřit, zda je odesílatel zprávy důvěryhodný. Je tedy nezbytně nutné v případě incidentu oznámeným odesílatelem označujícím se nebo vystupujícím jménem našeho zákazníka jeho autorizace, která je popsaná v interní směrnici bezpečnostního týmu. V případě oznámení incidentu třetí stranou je nutné ověřit důvěryhodnost odesílatele a incident samotný.

Klasifikace bezpečnostního incidentu
Je nutné každý bezpečnostní incident korektně klasifikovat dle znalostí a následně provést eskalaci pro konkrétní událost na základě známého postupu.
Všechny incidenty spravované CSIRT týmem MASTER.CZ-CSIRT by měly být klasifikované do jedné z kategorií z následující tabulky.

Kategorie incidentu	Úroveň rizika	Popis
Hlášení o spamu	1	Hlášení o nevyžádaném sdělení. Do této klasifikace spadá i žádost o vyřazení z newsletteru.
Hlášení o mailinglistu	2	Hlášení týkající se zahrnutí IP adresy z našeho rozsahu v blacklistech.
Bounce spam	1,2	Hlášení týkající se využití IP adres našeho rozsahu pro bounce spam.
Přicházející DoS a DDoS	3	Technika útoku na síťová zařízení, používaná pro znepřístupnění služby daného zařízení. Přicházející útok eskalovat na administrátory, který problém řeší. Nebere se v potaz útok zachycený plošnou antiDDoS ochranou.
Odcházející DoS a DDoS	3	Technika útoku na síťová zařízení, používaná pro znepřístupnění služby daného zařízení. Odcházející útok tohoto typu většinou naznačují napadané zařízení z našeho rozsahu a je nutné jej neprodlené řešit.
Porušení autorských práv	1,2	Sdílení materiálu, obsahu nebo neoprávněné zasáhnutí do zákonem chráněných práv autorského díla.

Phishing, pharming	2,3	Nástroje pro neoprávněné získání citlivých informací (hesla, kryptografické klíče atd.)
Scanning,cracking aplikací	2,3	Techniky sloužící k získání informací o síťových prostředcích a případnému zneužití síťových služeb nebo jejich prostředků.
Malware	3	Program sloužící pro vniknutí, využití nebo poškození počítačového systému (rootkit, infikovaný server).
Kompromitovaná aktiva	2,3	Zahrnuje kompromitovaného hosta, síťové zařízení, aplikaci nebo uživatelský účet. Do této kategorie patří i infikovaný host, který je aktivně ovládán útočníkem.
Otevřený DNS, NTP server	1,2	Pomocí otevřených DNS, NTP serverů je možné vykonávat tzv. "Amplification" útoky. Je tedy nutné řešit se zákazníky a zejména nepoužívat name servery s otevřenými rekurzemi.
Kompromitované informace	3	Úspěšný pokus o zničení, narušení nebo změnu citlivých údajů.
Porušení zákonů ČR	3	Vydírání, podvody a ostatní aktivity, které jsou v rozporu se zákony České republiky.
ostatní	1,2,3	Ostatní bezpečnostní incident konzultovaný s ostatními členy CSIRT týmu.

*úroveň rizika závisí na okolnostech.

Opatření
Jednotlivé kroky opatření se řídí na základě dvou hlavních kritérií – pokud se jedná o bezpečnostní incident směřující od nebo na aktiva v naší správě nebo jde o aktiva ve správě našich zákazníků.

a) **Aktiva v naší správě**: eskalace problému na majitele / administrátory spoléhající za chod tohoto aktiva. Zpravidla se jedná o servery / službu v naší správě. Bezpečnostní incidenty předáváme rovnou administrátorům spravující daný server / službu (kontaktní email: managed@master.cz)

b) **Aktiva ve správě zákazníků**: kontaktování a eskalace bezpečnostního incidentu na majitele daného aktiva (služba / server / rozsah IP adres...). Viz. Interní směrnice MasterDC s.r.o. pro technickou podporu.
Dle klasifikace bezpečnostního incidentu provedeme úkon korespondující s úrovní rizika daného incidentu.

Postup a eskalace dle kategorie incidentu

Každý incident je nutné třídit dle subjektu (vlastníka), kterého se týká a dle toho postupovat. Při provádění opatření pro "Aktiva v naší správě" vždy předat vytvořený ticket pro daný incident na managed@master.cz a dle úrovně rizika kontaktovat administrátora, který problém bude řešit. Počty hlášení / stížností nebo zjištění jsou vždy brány v potaz v intervalu 24 hodin. Pokud těchto stížností chodí markantně více, tak je nutné rovnou přejít k dalšímu bodu postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Hlášení o spamu	1	Přeposlání stížnosti majiteli s vlastním komentářem daného nahlášení.
	2	Přeposlání stížnosti majiteli s upozorněním na opakující se hlášení daného incidentu.
	3	Volání vlastníkovi bezpečnostního incidentu s upozorněním na možnou blokaci služeb z naší strany do vyřešení problému a požadavek na vyjádření do vytvořeného ticketu.
	4 a více	Blokace SMTP portu dané služby, u které dochází k bezpečnostnímu incidentu.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti týkající se stejného rozsahu / schránky daného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Hlášení mailinglistu	1	Přeposlání stížnosti majiteli s vlastním komentářem daného hlášení.
	2	Volání vlastníkovi bezpečnostního incidentu s upozorněním a požadavek na vyjádření do vytvořeného ticketu.
	3	Volání vlastníkovi s upozorněním na možnou blokaci služeb z naší strany do vyřešení problému a urgovat požadavek na vyjádření do vytvořeného ticketu.
	4 a více	Blokace SMTP portu dané služby, u které dochází k bezpečnostnímu incidentu.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah / schránku u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Bounce spam	1	Přeposlání stížnosti majiteli s vlastním komentářem k dané stížnosti na bounce spam z našeho rozsahu.
	2	Přeposlání stížnosti majiteli s upozorněním na opakující se hlášení týkajícího se bounce spamu.
	3	Volání vlastníkovi s upozorněním na možnou blokaci služeb z naší strany do vyřešení problému a požadavek na vyjádření do vytvořeného ticketu, kde se bezpečnostní incident řeší.
	4 a více	Blokace SMTP portu dané služby, u které dochází k bezpečnostnímu incidentu.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Přicházející DoS a DDoS	1	Omezení příchozího provozu na cílové IP adresy útoku. Zaslání zákazníkovi upozornění o omezení provozu.
	2	Blokace příchozího provozu na cílové IP adresy útoku. Zaslání zákazníkovi upozornění o blokaci.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Odcházející DoS a DDoS	1	Omezení odchozího provozu zdrojové IP adresy útoku. Zaslání zákazníkovi upozornění o omezení provozu.
	2	Blokace odchozího provozu zdrojové IP adresy útoku. Zaslání zákazníkovi upozornění o blokaci.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Porušení autorských práv	1	Přeposlání stížnosti majiteli s vlastním komentářem daného hlášení.
	2	Přeposlání stížnosti majiteli s upozorněním na opakující se porušování autorských práv.
	3	Volání vlastníkovi s upozorněním na možnou blokaci služeb z naší strany do vyřešení problému a požadavek na vyjádření do vytvořeného ticketu.
	4 a více	Blokace HTTP portu dané služby, u které dochází k porušování autorských práv.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Phishing, pharming	1	Přeposlání stížnosti majiteli s vlastním komentářem daného hlášení.
	2	Volání vlastníkovi s upozorněním na možnou blokaci služeb z naší strany do vyřešení problému a požadavek na vyjádření do vytvořeného ticketu.
	3 a více	Blokace HTTP portu dané služby, na které se nachází podvodné stránky.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Scanning, cracking aplikací	1	Přeposlání stížnosti majiteli s vlastním komentářem daného hlášení.
	2	Volání vlastníkovi s upozorněním na možnou blokaci služeb z naší strany do vyřešení problému a požadavek na vyjádření do vytvořeného ticketu.
	3 a více	Blokace odchozího provozu zdrojové IP adresy útoku. Zaslání zákazníkovi upozornění o blokaci.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Malware	1	Přeposlání stížnosti majiteli s vlastním komentářem daného hlášení.
	2	Volání vlastníkovi s upozorněním na možnou blokaci služeb z naší strany do vyřešení problému a požadavek na vyjádření do vytvořeného ticketu.
	3 a více	Blokace HTTP portu dané služby, na které se nachází malware.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Kompromitovaná aktiva	1	Přeposlání stížnosti majiteli s vlastním komentářem daného hlášení.
	2	Volání vlastníkovi s upozorněním na možnou blokaci služeb z naší strany do vyřešení problému a požadavek na vyjádření do vytvořeného ticketu.
	3 a více	Blokace kompromitované služby.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Otevřený DNS, NTP server	1	Přeposlání stížnosti majiteli s vlastním komentářem daného hlášení.
	2	Přeposlání stížnosti majiteli s upozorněním na opakující se hlášení daného incidentu.
	3	Volání vlastníkovi bezpečnostního incidentu s upozorněním na možnou blokaci služeb z naší strany do vyřešení problému a požadavek na vyjádření do vytvořeného ticketu.
	4 a více	Blokace DNS, NTP portu dané služby, na které se nachází otevřený DNS, NTP server.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Kompromitované informace	1	Přeposlání stížnosti majiteli s vlastním komentářem daného hlášení.
	2	Volání vlastníkovi s upozorněním na možnou blokaci služeb z naší strany do vyřešení problému a požadavek na vyjádření do vytvořeného ticketu.
	3 a více	Blokace kompromitované služby.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Typ incidentu	Počet hlášení / stížností / zjištění	Postup
Porušení zákonů ČR	1	Přeposlání stížnosti majiteli s vlastním komentářem daného hlášení a upozorněním na možnou blokaci služeb z naší strany do vyřešení problému.
	2	Volání vlastníkovi s upozorněním na možnou blokaci služeb z naší strany do vyřešení problému a požadavek na vyjádření do vytvořeného ticketu.
	3 a více	Blokace služby, která porušuje zákony ČR.

Pokud dojde k reakci zákazníka na vytvořený ticket s řešením daného problému, tak je možné případ považovat jako vyřešený. Pokud dojde k další stížnosti na stejný rozsah u stejného zákazníka, postupujeme vždy o jednu úroveň výše uvedeného postupu.

Archivace
Jednotlivé bezpečnostní incidenty jsou archivovány v ticketovacím systému RT. Evidence a archivace je vedena dle subjektu, které se daný incident týká a čísla ticketu konkrétního incidentu.

Užitečné nástroje

-pro případné prověření oznámení o incidentu lze použít různé nástroje, které mohou potvrdit daný incident případně daný nástroj použít jako prevenční nástroje.

Skener webu
-skenování bezpečnosti stránek zdarma
- www.skenerwebu.cz

Test pro mailservery
-kompletní test IP mailserveru a jeho listingu v rámci mnoha blacklistů (RBL / DNSBL)
- http://multirbl.valli.org/lookup/
- u každého listingu je nutné pročíst poznámku – některé blacklisty jsou zastaralé nebo nadále nevyužívané

Vyhledávání kontaktních informací
-Vyhledání správného kontaktu patří mezi nejdůležitější části hlášení bezpečnostních incidentů
- https://apps.db.ripe.net/search/query.html
- http://whois.domaintools.com/