Bezpečnostní incidenty

Provozovatel internetových služeb (dále jen „Provozovatel") je živnostník Michal Dohnálek, IČ: 0999296, se sídlem Náves 73, 66408 Blažovice. Společnost je zapsána v obchodním rejstříku vedeném Krajským soudem v Ostravě oddíl C, vložka 87619.

Definice bezpečnostního incidentu

Bezpečnostním incidentem je označení nestandartní či nepříjemné bezpečnostní události, která vede k narušení bezpečnosti sítě hostingu nebo poškození sítě poskytovatele, nebo subdodavatele.

Řešení problémů

V případě, že dojde stížnost na IP adresu přiřazenou serveru zákazníkovi, poskytovatel standardně provede následující kroky:

1. Ověří důvěryhodnost odesílatele stížnosti, případně si vyžádá další potřebné informace k vyřešení incidentu.
2. Pokud došlo k úspěšnému ověření důvěryhodnosti odesílatele poskytovatel přeposílá stížnost zákazníkovi a požaduje odstranění problému.
3. Pokud zákazník si neví rady s vyřešením problému je oprávněn požádat o pomoc poskytovatele
4. V případě, že je problém vyřešen, požadavek se uzavře.
5. Pokud zákazník neodpoví do vyžadované doby provozovatel je oprávněn dočasně pozastavit síť, bez náhrady na kompenzaci škod, způsobené pozastavením sítě.

Vyžadována reakční doba:

Každý zákazník nesmí způsobit více jak 3 bezpečnostní incidenty během 30 dní.

- Vyžadována reakční doba, do které musí zákazník odpovědět, vyjádřit se k bezpečnostnímu incidentu a vyřešit ho se stupňuje dle počtu incidentů za měsíc.
- V případě třetí stížnosti během 30 dnů provozu je poskytovatel oprávněn udělit postih. Výše postihu je specifikována v tabulce "Postihy za 3. stížnost během 30 dní".

Vyžadována reakční doba - 1. stížnost během 30 dní

Úroveň	Riziko	Typický incident	Vyžadována reakce*
1	Nízké	Spam	24 hodin
2	Střední	Odchozí bruteforce	12 hodin
3	Vysoké	Odchozí DDoS	30 minut

Vyžadována reakční doba - 2. stížnost během 30 dní

Úroveň	Riziko	Typický incident	Vyžadována reakce*
1	Nízké	Spam	12 hodin
2	Střední	Odchozí bruteforce	6 hodin
3	Vysoké	Odchozí DDoS	20 minut

**Do doby uvedené v tabulce je zákazník povinen odpovědět na výzvu poskytovatele k vyřešení bezpečnostního incidentu a podání vyjádření.*

Postihy za 3. stížnost během 30 dní

Úroveň	Riziko	Typický incident	Postih*
1	Nízké	Spam	Dle uvážení podpory
2	Střední	Odchozí bruteforce	POZASTAVENÍ SÍTĚ PO DOBU 72 HODIN
3	Vysoká	Odchozí DDoS	POZASTAVENÍ SÍTĚ PO DOBU 168 HODIN

**Poskytovatel je oprávněn upravit výši postihu dle vážnosti incidentu a spolupráce během řešení. Pokud má zákazník prokazatelnou snahu vyřešit problém, poskytovatel postih udělit dle uvážení nemusí.*

Security Incidents

The operator of online services (hereinafter referred to as the "Operator") is a self-employed person Michal Dohnálek, ID No.: 0999296, with registered office at Náves 73, 66408 Blažovice. The company is registered in the Commercial Register maintained by the Regional Court in Ostrava, Section C, Insert 87619.

Definition of a security incident

A security incident is the designation of a non-standard or unpleasant security event that leads to a disruption of the security of the hosting network or damage to the network of the provider or subcontractor.

Problem solving

In the event of a complaint to an IP address assigned to a customer's server, the provider will normally take the following steps:

1. *Verifies the credibility of the complainant, or requests other necessary information to resolve the incident.*
2. *If the credibility of the sender has been successfully verified, the provider forwards the complaint to the customer and requests that the problem be resolved.*
3. *If the customer is unable to resolve the problem, he is entitled to ask the provider for assistance.*
4. *If the problem is resolved, the request is closed.*
5. *If the customer fails to respond within the required time, the operator is entitled to temporarily suspend the network, without compensation for damages caused by the suspension of the network.*

Required response time:

Each customer must not cause more than 3 security incidents within 30 days.

- *The required response time within which the customer must respond, comment on the security incident and resolve it increases with the number of incidents per month.*
- *In the event of a third complaint within 30 days of operation, the provider is entitled to impose a penalty. The amount of the penalty is specified in the table "Penalties for the 3rd complaint within 30 days".*

Required response time - 1st complaint within 30 days

Úroveň	Riziko	Typický incident	Vyžadována reakce*
1	Low	Spam	24 Hours
2	Medium	Outgoing bruteforce	12 Hours
3	Hight	Outgoing DDoS	30 minutes

Required response time - 2nd complaint within 30 days

Úroveň	Riziko	Typický incident	Vyžadována reakce*
1	Low	Spam	12 Hours
2	Medium	Outgoing bruteforce	6 Hours
3	Hight	Outgoing DDoS	20 minutes

**The customer is obliged to respond to the provider's call to resolve the security incident and submit a statement within the time specified in the table.*

Penalties for the 3rd complaint within 30 days

Úroveň	Riziko	Typický incident	Postih*
1	Low	Spam	At the discretion of support
2	Medium	Outgoing bruteforce	NETWORK SUSPENSION FOR 72 HOURS
3	Hight	Outgoing DDoS	NETWORK SUSPENSION FOR 168 HOURS

**The provider is entitled to adjust the amount of the penalty according to the seriousness of the incident and cooperation during the resolution. If the customer has demonstrable efforts to resolve the problem, the provider may decide not to impose the penalty.*