CSIRT DATASPRING TÝM SPOLEČNOSTI AUTOCONT A.S.

1. O tomto dokumentu

Tento dokument obsahuje údaje, týkající se řešení bezpečnostních incidentů ve společnosti AUTOCONT a.s. Je koncipován podle standardu RFC 2350. Poskytuje základní informace o týmu CSIRT DataSpring, možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

1.1. Datum poslední aktualizace

Toto je verze číslo 2 ze dne 21. 3. 2022

1.2. Distribuční seznam pro oznámení

Distribuční seznam pro oznámení není veřejný.

1.3. Místa, kde může být tento dokument nalezen

Aktuální verze tohoto popisného dokumentu je dostupná na internetové stránce
www.autocont.cz/dcs/kontakty

2. Kontaktní informace

2.1. Název týmu

CSIRT DataSpring

2.2. Adresa

CSIRT DataSpring
AUTOCONT a.s.
Vinohradská 230
100 00 Praha 10
Česká republika

2.3. Časové pásmo

SEČ, Středoevropský čas (UTC +1, od poslední neděle v říjnu do poslední neděle v březnu)
SELČ, Středoevropský letní čas (UTC +2, od poslední neděle v březnu do poslední neděle v říjnu)

2.4. Telefonní číslo

+420 222 74 40 13

2.5. Ostatní telekomunikace

Není k dispozici.

2.6. Elektronická adresa

Pro komunikaci, prosím, použijte adresu abuse@dataspring.cz

2.7. Veřejné klíče a šifrovací informace
Pro ověřování emailů se používá S/MIME.
Informace o certifikační autoritě:
Common Name: AutoCont CA2
SHA:256:92:3A:0C:CF:1A:B1:ED:5C:55:45:97:90:BB:2A:D3:3A:10:60:2C:2C:7B:8D:
FC:CE:D3:02:28:C5:E4:32:EA:60
SHA-1: 18:B8:16:37:C8:D6:CE:91:7B:2E:34:27:0E:9A:C6:3E:65:19:3C:69

2.8. Členové týmu
Kompletní přehled členů týmu CSIRT DataSpring není veřejně k dispozici.

2.9. Další informace
Není k dispozici.

2.10. Kontakt s veřejností
Preferovaný způsob kontaktování CSIRT DataSpring je prostřednictvím e-mailu. Hlášení incidentů a související otázky zasílejte na adresu abuse@dataspring.cz. Není-li možné použít e-mail, můžete CSIRT DataSpring kontaktovat telefonicky na výše uvedeném čísle. Tým CSIRT DataSpring může být kontaktován 24/7/365.

3. Stanovy
3.1. Poslání
CSIRT DataSpring řeší bezpečnostní incidenty zjištěné v rámci provozovaných sítí a systémů divize DCS společnosti AUTOCONT a.s. a jejích zákazníků.

3.2. Cílová skupina
Naší cílovou skupinou jsou obchodní partneři divize DCS společnosti AUTOCONT a.s., zejména zákazníci, instituce veřejného sektoru, ISP, dále pak organizace a jednotlivci ovlivnění anebo ovlivňující činnosti naše či našich zákazníků.

3.3. Zařazení
Tým CSIRT DataSpring je součástí organizační struktury divize DCS společnosti AUTOCONT a.s. a funguje zejména v procesu Incident Management v rolích zajišťujících převzetí, evidenci, řešení, sledování, komunikaci a vyhodnocování bezpečnostních incidentů.

3.4. Oprávnění
CSIRT DataSpring pracuje v mezích české legislativy. CSIRT DataSpring při řešení incidentů spolupracuje se správci systémů zákazníků, partnerů a s dalšími uživateli v rámci institucí veřejného sektoru a ISP, případně s ostatními osobami ovlivněnými činností naší a našich zákazníků CSIRT DataSpring se řídí interními směrnicemi a procesy divize DCS společnosti AUTOCONT a.s., které vyplývají z funkcí ISMS systému a požadavky normy ISO27001 a dalších.

4. Zásady
4.1. Typy incidentů a úroveň podpory
Bezpečnostní incident znamená nestandardní bezpečnostní událost, která způsobila narušení důvěrnosti, integrity, dostupnosti či neodmítnutelnosti informací či zařízení, a to v důsledku selhání

nebo porušení bezpečnostních opatření. CSIRT DataSpring řeší bezpečnostní incidenty, které vznikly, trvají, anebo můžou potenciálně vzniknout, v rámci ASN 201730 a služeb, poskytovaných divizí DCS společností AUTOCONT a.s.
Úroveň podpory poskytnuté CSIRT DataSpring při řešení bezpečnostního incidentu se liší v závislosti na typu a závažnosti incidentu (jeho dopadu – míry narušení poskytovaných služeb, resp. v případě, že vektor útoku vychází z prostředí DataSpring, pak také míra účinku působení takového útoku na okolí), na oznamovateli a postižené straně.
CSIRT DataSpring pro řešení bezpečnostních incidentů má zpracován a zaveden proces Incident Management a dle tohoto procesu uvolní k řešení incidentu zdroje adekvátní konkrétnímu incidentu.
CSIRT DataSpring bude dle svých možností proaktivně informovat interní struktury divize DCS společnosti AUTOCONT a.s. a její zákazníky o potenciálních hrozbách a zjištěných zranitelnostech ještě před jejich možným zneužitím.

4.2. Spolupráce, interakce a zpřístupňování informací

CSIRT DataSpring je připraven spolupracovat s ostatními bezpečnostními týmy. S informacemi získanými v rámci činnosti CSIRT DataSpring nebo sdílenými v rámci komunity bezpečnostních týmu je nakládáno v souladu s požadavky české a evropské legislativy.

4.3. Komunikace a autentizace

E-maily a telefony jsou považovány za dostatečně bezpečný způsob, použitelný nešifrovaně, při přenosu málo citlivých dat. Informace o ověřování a šifrování naleznete v sekci 2.7.

5. Služby

5.1. Reakce na incidenty

CSIRT DataSpring bude aktivně vystupovat při řešení technických a organizačních aspektů bezpečnostních incidentů, u kterých je to z charakteru incidentu možné. Na řešení ostatních typů incidentu bude spolupracovat. Bude poskytovat odbornou pomoc s následujícími typy činností:

5.1.1. Třídění incidentů

Posouzení, zda je incident věrohodný. Určení rozsahu incidentu a jeho priority.

5.1.2. Koordinace při řešení incidentu

Kontaktování zúčastněných stran incidentu k prošetření incidentu a následné přijetí příslušných opatření. Usnadnění kontaktu s dalšími subjekty, které mohou pomoci s řešením incidentu. Informování ostatních CERT a CSIRT týmů v případě potřeby. Komunikace se zúčastněnými stranami.

5.1.3. Řešení incidentu

Aktivní řešení incidentu. Vytvoření, testování a nasazení řešení (případně dočasného řešení) zamezující zjištěnému narušení bezpečnosti aktiv. Realizace nápravných opatření zamezujících opakování incidentu.

5.2. Proaktivní přístup

CSIRT DataSpring provádí pravidelnou analýzu rizik s cílem minimalizovat míru rizika působící na informační aktiva – cestou snižování zranitelností těchto aktiv, případně vhodným omezením hrozeb působících na tato aktiva. Pro potřeby zásahu se používají bezpečnostní kontakty předané zákazníky a obchodními partnery. CSIRT DataSpring zvyšuje povědomí o bezpečnosti u svých zákazníků.

CSIRT DataSpring se zabývá shromažďování údajů o událostech, které by mohly mít dopad na bezpečnost v sítích divize DCS společnosti Autocont a.s. a jejích zákazníků.

6. Zproštění odpovědnosti

CSIRT DataSpring i přes veškerou svou odbornost, zavedené procesy a opatření nemůže garantovat, že veškeré výstupy budou vždy zcela bezchybné, včasné a zcela zabrání škodě nebo žádnou škodu nezpůsobí. CSIRT DataSpring dále v dobré víře může spoléhat na informace od zákazníka nebo jiné třetí strany, které se mohou ukázat nepřesné, mylné, zavádějící či jiným způsobem závadné, důsledkem čehož může dojít k vadám nebo vzniku škod. Příjemce je povinen si obdržené výstupy vždy pečlivě zkontrolovat a sám odborně vyhodnotit. V případě jakéhokoliv nesouhlasu nebo pochybností ohledně výstupů je povinen činnost neprovádět, případně okamžitě zastavit a CSIRT DataSpring ihned kontaktovat. V opačném případě AUTOCONT a.s. nenese za výstupy jakoukoliv odpovědnost, zejména za případné chyby, opomenutí či škody vyplývající z využití informací ve výstupech.