Void

EKI Report

Ukážka pre spoločnosť Neznámy s.r.o.

Void

Vstupné informácie

meno.priezvisko@neznamy.sk

Sieťové informácie

Prvým krokom pri pohľade na kybernetickú bezpečnosť Vašej spoločnosti je zmapovanie základných sieťových informácií o nej. Sú verejné dostupné na internete a sú potrebné, aby systémy ostatných užívateľov a firiem s tými Vašimi vôbec vedeli komunikovať.
Na druhej strane, toto sú zároveň informácie s ktorými pracujú aj útočníci a môžu ich využiť na to, aby sa o Vašich systémoch dozvedeli cenné detaily o ich ochrane. Čím menej takýchto informácií budete na internete publikovať, tým ťažšiu prácu budú mať.

Vaše verejné IP adresy:

291.995.144.0 - 912.995.945.255, 89.352.7.430

DNS Servery:

ns1.neznamy.sk.	291.995.145.200	ASxxxx Neznamy, krajina
ns2.neznamy.sk.	291.995.145.201	ASxxxx Neznamy, krajina

Host záznamy:

ns1.neznamy.ro	291.995.145.200	ASxxxx Neznamy, krajina
ns2.neznamy.ro	291.995.145.201	ASxxxx Neznamy, krajina
mpx-web.neznamy.ro	291.995.145.205	ASxxxx Neznamy, krajina
threatgrid.neznamy.ro	291.995.144.44	ASxxxx Neznamy, krajina
expe.neznamy.ro	291.995.145.193	ASxxxx Neznamy, krajina
vmdmm.neznamy.ro	291.995.145.131	ASxxxx Neznamy, krajina
xmpp.neznamy.ro	291.995.145.198	ASxxxx Neznamy, krajina
aw.neznamy.ro	291.995.145.194	ASxxxx Neznamy, krajina
dns-fw.neznamy.ro	291.995.145.241	ASxxxx Neznamy, krajina
mpx.neznamy.ro	291.995.145.204	ASxxxx Neznamy, krajina
mx.dnss.neznamy.ro	291.995.145.202	ASxxxx Neznamy, krajina
mx.datanets.ro	291.995.145.202	ASxxxx Neznamy, krajina
dnss.neznamy.ro	291.995.145.200	ASxxxx Neznamy, krajina
proxy1-mgmt.neznamy.ro	291.995.145.203	ASxxxx Neznamy, krajina
www.neznamy.ro	289.935.37.130	ASxxxx Neznamy, krajina
apps.neznamy.ro	291.995.145.196	ASxxxx Neznamy, krajina
ns1.neznamy.ro.	291.995.145.200	ASxxxx Neznamy, krajina
ns2.neznamy.ro.	291.995.145.201	ASxxxx Neznamy, krajina
mx.neznamy.ro.	291.995.145.202	ASxxxx Neznamy, krajina

Void

Otvorené porty:

Porty sú konkrétne rozhrania, prostredníctvom ktorých systémy medzi sebou komunikujú. Otvorené porty sú tie, na ktorých "počúvajú," čiže sú prístupné pre komunikáciu zvonka. Je dôležité, aby systémy v tomto zozname boli dobre zabezpečené a nenachádzali sa tam žiadne služby a porty o ktorých neviete.

291.995.145.242	443/TCP/HTTPS
291.995.145.244	443/TCP/HTTPS
291.995.145.200	53/UDP/DNS
291.995.145.202	25/TCP/SMTP
291.995.145.193	443/TCP/HTTPS, 5060/UDP/SIP, 5222/TCP/xmpp, 8443/TCP/HTTPS
291.995.145.241	443/TCP/HTTPS
291.995.145.247	25/TCP/SMTP
291.995.145.246	25/TCP/SMTP
289.935.37.130	21 26 53 80 110 143 443 465 587 993 995 2082 2083 2087 2095

Void

Zraniteľnosti:

Zraniteľnosti v ponímaní kybernetickej bezpečnosti sú konkrétne slabé miesta, ktoré môžu byť zneužité útočníkom alebo škodlivým softvérom pre získanie kontroly nad daným systémom a jeho poškodenie, zničenie alebo iné neautorizované aktivity.
Zraniteľnosti sú často zverejňované samotnými výrobcami HW a SW pri vydávaní nových verzií, ktoré ich zároveň odstraňujú. Preto, čím dlhšiu dobu nie sú systémy aktualizované, tým viac známych zraniteľností sa ich týka a tým väčšie je riziko ich zneužitia.

Nájdené známe zraniteľnosti:

291.995.145.242 Apache 2.4.1,

CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.
CVE-2017-15715	In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.
CVE-2013-6438	The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.
CVE-2012-2687	Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2012-4558	Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.
CVE-2012-3499	Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.
CVE-2018-17199	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
CVE-2013-2249	mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.
CVE-2017-9788	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
CVE-2014-8109	mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.
CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
CVE-2017-9798	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
CVE-2012-0883	envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.
CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
CVE-2016-2161	In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.
CVE-2014-0231	The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2016-8743	Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

Void

Náhľad na bezpečnosť Vašej domény - neznamy.sk

V tejto sekcii nájdete základný prehľad bezpečnostných opatrení troch dôležitých oblastí, ktoré pri komunikácií cez internet využíva každá organizácia.
Každé opatrenie, ktoré nie je označené zeleným indikátorom, predstavuje zvýšené kybernetické riziko, ktorému je Vaša firma vystavená. Ako dané opatrenie implementovať a príslušné riziko zmierniť, skonzultujte so svojim IT špecialistom alebo využite niektoré z našich služieb.

Domain

- ✓ Name servers
- ✗ DNSSEC
- ✗ CAA

Email

⚠ Mail servers

SECURE TRANSPORT (SMTP)

- ✓ TLS
- ⚠ Certificates
- ✗ MTA-STS
- ✗ TLS-RPT
- ✗ DANE

AUTHENTICATION AND POLICY

- ✓ SPF
- ✗ DMARC

WWW

PROTOCOLS

- ✓ HTTP (80)
- ✓ HTTPS (443)

SECURE TRANSPORT

- ✓ TLS
- ✓ Certificates
- ✓ Cookies
- ✓ Mixed Content

MODERN SECURITY FEATURES

- ✗ Strict Transport Security
- ✗ Content Security Policy
- ✗ Subresource Integrity
- ✗ Expect CT

APPLICATION SECURITY

- ✗ Frame Options
- ✗ XSS Protection
- ✗ Content Type Options

V̄oıd

Úniky dát

Ak ste Vaše údaje použili pri registrácii v niektorej zo služieb na internete, a tá sa stala predmetom kybernetického útoku, je možné že tieto informácie o Vás boli súčasťou dát, ktoré sa dostali do nepovolaných rúk. Predstavuje to riziko vo viacerých rovinách - ak ste napríklad rovnaké heslo použili aj pri inej službe, môžu ho útočníci použiť pre získanie prístupu aj k nej. Alebo, môžu zozbierané informácie využiť pre vytvorenie falošnej identity a vykonávanie nekalých činností vo Vašom mene.

Emailová adresa: meno.priezvisko@neznamy.sk bola zistená v nasledovných únikoch dát:

Onliner Spambot

- August 2017
- Kompromitované dáta: email adresa, heslo

Apollo

- Júl 2018
- Kompromitované dáta: email adresa, zamestnávateľ, geografická lokácia, pracovná pozícia, Meno, Tel.číslo, Profily na sociálnych médiach

Collection #1 (unverified)

- Január 2019
- Kompromitované dáta: email adresa, heslo

Void

www.voidsoc.com
info@voidsoc.com