Baden-Württemberg

LANDESAMT FÜR VERFASSUNGSSCHUTZ

LfV BW · Postfach 50 07 00 · 70337 Stuttgart

[redacted]

Stuttgart
Durchwahl 0711 9544-
Name
Aktenzeichen
(Bitte bei Antwort angeben)

[redacted]

Warnmeldung über aktuelle Cyberangriffe gegen Unternehmen / Einrichtungen aus dem Gesundheitswesen

Anlage
Technische Indikatoren

Sachverhalt

Das Landesamt für Verfassungsschutz Baden-Württemberg (LfV BW) informiert Sie hiermit über eine aktuelle Cyberangriffswelle gegen Unternehmen / Einrichtungen aus dem Gesundheitssektor. Konkrete Hinweise auf eine Betroffenheit baden-württembergischer Einrichtungen des Gesundheitswesens liegen dem LfV BW derzeit jedoch noch nicht vor. Hinter dem Angriff wird eine nachrichtendienstlich gesteuerte Angreifergruppierung vermutet.

Mögliche Angriffsvektoren

Spear-Phishing-Mails

- Zielgerichteter, glaubhaft erscheinender Versand von E-Mails an Mitarbeiter, die u.a. maliziöse Anhänge oder Links enthalten könnten.

Watering-Hole-Attacken

- Schadsoftware oder Phishing-Links werden durch die Angreifer gezielt auf legitimen Webseiten platziert, die für die Unternehmen / Einrichtungen interessant sein könnten.

Ausnutzen von Schwachstellen in Software- oder Hardwareeigenschaften

- Bekannte oder unbekannte Schwachstellen werden ausgenutzt, um Schadsoftware im Opfersystem zu implementieren

Handlungsempfehlungen

Für IT-Verantwortliche:

- Prüfen Sie Ihre Netzwerk-Logs auf die in der Anlage aufgeführten technischen Indikatoren. Sind ungewöhnliche Verbindungen feststellbar?
- Befinden sich Ihre Software- bzw. Hardwareeigenschaften auf dem aktuellen Stand (siehe ausgenutzte Schwachstellen im Anhang)?
- Sensibilisierung der Mitarbeiter

Für Mitarbeiter:

- Achten Sie auf verdächtige E-Mails und prüfen diese auf Plausibilität („Erwarte ich eine solche E-Mail? Ist der Kontext plausibel?“). Melden Sie verdächtig aussehende E-Mails Ihrem IT-Sicherheitsbeauftragten.
- Vermeiden Sie bei verdächtig erscheinenden E-Mails Anhänge oder Links anzuklicken und dort ggf. Passwörter oder Zugangsdaten preiszugeben.

Bei einer verdächtigen Trefferlage bitten wir Sie das Landesamt für Verfassungsschutz Baden-Württemberg zu informieren. Hierbei kann Ihnen von Seiten der Verfassungsschutzbehörden Vertraulichkeit zugesichert werden.

[redacted]

Anhang – Technische Indikatoren

Netzwerkbasierte Indikatoren

E-Mail-Adressen
nksis12@nate[.]com
taeyang2911@daum[.]net

IP-Adressen
174.142.90[.]208
211.255.32[.]175
183.63.53[.]219
95.110.201[.]160
5.77.54[.]18
67.222.157[.]160

Domains
cgalim[.]com
hakproperty[.]com
0756rz[.]com
10vs[.]net
168va[.]com
1996hengyou[.]com
51xz8[.]com
hypnosmd[.]com
computer[.]case
control[.]in
hmamail[.]com
organization[.]in
partitions[.]it
path[.]in
foodforu.heliohost[.]org

URLs
hxxp://hakproperty[.]com/new/plat/pu.php?do=download_rc&aid=
hxxp://cgalim[.]com/admin/hr/1.apk
hxxp://hakproperty[.]com/new/plat/pu.php?do=upload
hxxp://cgalim[.]com/admin/1211me/Ant_3.5.exe
hxxp://cgalim[.]com/admin/1211me/Servlet.exe
hxxp://cgalim[.]com/admin/1211me/desktops.ini
hxxp://cgalim[.]com/admin/hr
hxxp://cgalim[.]com/admin/hr/hr.doc
hxxp://cgalim[.]com/admin/hr/temp.set
hxxp://ebsmpi[.]com/ipin/360/ant_3.5.exe
hxxp://ebsmpi[.]com/ipin/360/ant_4.5.exe
hxxp://ebsmpi[.]com/ipin/360/desktops.ini
hxxp://ebsmpi[.]com/ipin/360/down.php
hxxp://0756rz[.]com/

hxxp://168va[.]com/include/data/left.php
hxxp://1996hengyou[.]com/include/dialog/left.php
hxxp://51xz8[.]com/include/top.php
hxxp://hypnosmd[.]com/include/top.php
hxxp://artndesign2.cafe24[.]com:80/skin_board/s_build_cafeblog/exp_include/img.png
hxxp://path[.]in
hxxp://path.in/
hxxp://organization[.]in/
hxxp://foodforu.heliohost[.]org/blog/apache.jpg
hxxp://discgolfglow[.]com/wp-content/uploads/2015/08/image-blog4-518x343.jpg
hxxp://discgolfglow[.]com/wp-content/uploads/2015/08/ipp.conf
hxxp://www.edsi[.]co.kr/admin/main_page/photo/data/erphoto.small
hxxp://foodforu.heliohost[.]org/blog/adata/784561C6/20170712075823.apk
hxxp://foodforu.heliohost[.]org/blog/adata/040CCEDA/20170711195147.apk
hxxp://www.kohtao-idc[.]com/wp-includes/kernelos.jpg
hxxp://station.brinkleyspubs[.]com/wp-includes/body.swf
hxxp://www.etgcx[.]com/common/image/bgirl.jpg
hxxp://foodforu.heliohost[.]org/blog/adata/48D224FF/20170708000822.apk
hxxp://foodforu.heliohost[.]org/blog/adata/784561C6/20170709062859.apk
hxxp://www.imuz[.]com/admin/data/bbs/review2/board/170B10FB_put.jpg
hxxp://www.kohtao-idc[.]com/wp-includes/hashtag.jpg
hxxp://www.korea-tax[.]info/crossdomain.xml
hxxp://www.portmultimedia[.]com/wp-includes/wpdict.jpg
hxxp://nejebad[.]com/images/statusicon/post_old.gif
hxxp://station.brinkleyspubs[.]com/wp-includes/point.jpg
hxxp://foodforu.heliohost[.]org/blog/adata/B8975A85/20170711013719.apk
hxxp://www.chateau-eu[.]fr/wp-content/player/qq3.swf

Hostbasierte Indikatoren

MD5
f5cae9fcc8bad42b3dddb71ce68dbd92
ab4596f26b25730fbc9dc41e629980f1
eede299ee7f6c0637d59f0139b8d2940
237ff78e9d8c9407f89563cb696c2539
fed4b7096553965a07e0f340494889fe
8842e183d4b2cf5fb8d0df7ee58d704a
3adcee3cdb6e21ca3427fade92a4840f
f5463cd95632706cd7823bfea8fc118c
bdbabe7d5605c00d24d15e3fac6eda1e
9ef215b13d1e0140ac563d6cdc7a1495
71c5990bd1c04488b3f99cbebbcbfc19
aab31132dfec1c82682b74f7277ad133

SHA-256
b80ca824b8a624cf48973a605c1253ebbab11df3da389e99814389e9884d1fbd
492745f34ed0ddef2c9a54aa7304bc0f478abe363dad3a498e94122436fa1405
5127cf9c236127e629b7ebf70a0b3d0672354338cf30efc4800444d16c3c710a

e3d4ef63aff0847d73267184eb5282ab5b34528a2d89dba315b75b2e618da386
bd3cfc12823f6ce9375f81396e6ec84a82c7f1aa4e4c28b21e0cf9d73e9f10c4
b59a8766fbd9e94c51a9cb8d651a72a0002846d56769a4c77b0b9404ad0d7765
efa9f75ee1f6804d1021fa203f17fb6129ca1634f3239746066ef773a49c11c0
af8016102c641686e0d3b34fe43bea60529585d81fdf59ad988369835e81a101
6a83e2f5a784cf317854079b6e24213b2769789f235c6999031a157c936b10c8
4ebcc28f7d96c1e440600deeea3002f59fe330a420e084239041989b2bf85ab0
21db3886f23e0829142327e0474349a178c22e57dc7dcbcccec0d770c3ab513c
cf7468d29cdf546783a3344d26b63fcce58100905e1a052ad942683e07b4da90
33891d153376168d0939419f3991c40f03cba32ad7cae0634adbd05abc887ff1
c89392fce7a2d6b65e67e51b66457e7893a928754f66a4619abc2ffde8a7a422
855fe90ecadfd74b20ca3b54d434f7329c267c7f4ff7c96c14efe5933c0831ca
6a436aca00171111e8bb3e66f0ebe48d0cc747f1a04932bb682b1f7494eab9e9
33ae3b40ea954477267675ddc5566b2ab784119ca6edb2041702d4f4b165fe33
3e4fa52f51f7702c0acf5431d5b23622b1199225d3438e1dadd46f078693e0c3
25fc24e92f480e527386c6c883e700513f17f884a857e04446c703def66fe3f4
f087c675749b8fcf851e17548f4c6986d40c8bbe6454837418bf3947f933275c
ddd974ed9a4d7c0ea63d0f5e0c4cdeec3071d82dc5980662ca234ef4379fdcb2
bded85d7024b6cf86cc9ce45ec851c80cb13790b9c4bd63b0b22b0fb672e9dce
8f8bedb89984c8e741e0e15f549a5c851b7e1d83c4179b306371e665b1a80147
6d1ce78b0d61fd94d41c927507ef497f25712199f812e582d2ef0c9c65feccca
94b55267821fcdc4b4e72708d6a404c1010af99e60a435e6bf748b6ccb40d7cb
b7a4bb1f60fb8abd60487388c4cdf890bb3030f95e1b4dca8ca4a571fcfd017d
4ae3b26d71d3a0524020e477c6d7e8473623c2eaa9a3ba8a946d582022d7cd59
a0359a6054ff3b245ca661ef5c51dd605410b946e1f0eff6f6898b2368b0ef7e
d31e3ca167784087aadb46700aaa6e4f2da2acfb5aaf36aea59af26030350040
50305b44e0bf97afdf14a746105fbb64c1879a91bcb2f4e932cbda14179e6713
0ac7b0a0a21ac576591a9a95daf08b6054fc4ccc2aad0a87fdae87ca9348dc8b
411ffd7f78bbc977f980e735d1facd49fdef0552fa55959d8cd4fe5138722955
aa127803f805a0c5b316e5d126f12d81b44032d82adfbdb4ecebec6dd7039d0a
c31700777fa417b6a95a18649aa0208cbaca947317914000426cb7c69ee12f50
1893af524edea4541c317df288adbf17ae4fcc3a30d403331eae541281c71a3c
3004196da6055c6f062c94a9aae8dc357fa19b953b071049083e69e840083cf9
14c58e3894258c54e12d52d0fba0aafa258222ce9223a1fdc8a946fd169d8a12
42cde9fd6f2fd70d6f6ccb4e03ccc9253ca99aae123d9ca6794243571930c744
17a5a22419f2f53fc92bf6964209e1bfc7f3c37b4f3fb90d65447b00d5ac1606
9326d68a93fbc73cdd54695b2ac835a297e9685506aaf692dd23dcda3e89d1d6
8a383fad84d672efe733b380eaa4777a7af9edce6f694cf1a183a0d645f048cc
329fda648701876ad67fe3a8f9608bbbf11af4cba603e67c9e66b103059ae19e
607dd23fcd70230dad540ddc43243edf0ca8687cd00a2dd984e109c79ab8d0ba
4cb0df1ede284aec9c28652a8ce60eae5fc5a34f297285c3bd2fc0640d120a46
2682193b4f6765e7d11bd0b6cecaeb1e67a845db1383986a17cc8a39540f732f
f440bbde112579f31553e02bf496ad1f7e31d59e4b485d1cb5b5cd776f4df864
a7141ce1a62f7e02b0bfe72ba122824915fcd7fe5cf02a2ed25b298965cfac41
42531dbf164652e88aec0104cb66ee7c4ebf18c5a1217cbbf396f8b7adacb71f
1cf81f35162c7a2625a8bef60e65f0bab207d8e0b48d34352a8c40e11bf78b62
589bb5b261c519774abcb38a8f511c0471747c156662b8dc84c7f14fdbf31c6a
77dfb4ac1cc7fd43f2e0b6a543a6502aa0c8019e7316d8e218b881ea028f3319

20dcbb43660456b39bcbb0e7ca65912f39692c9d1628fe09740ee5012e86a9db
0f22ccc4d0fbadfc480984ea4f1f8d754dd70d5a8877a60f59772cce6f028f45
f67ca424a1f5fbacc56f4280442923a50dd71a64a900b59c06d16b29adc04a0f
8c425eed76eab8a8509973e9c433cd821334c8b0dc67e83bcba62a529736ed25
4f07a1e7af7d6f274e7882efe1ea12db4f82b5f11e7ff687e2dbe02ea8dfe3cc
977245aa2c0d4a210622170311f6b8785fbd2d168171c804dbbf8fa6efa58ca0
d5f1897526aa656b65cdd53bf91fa21dc49d5942606d399c3bb2dcbce59954cd
5770875d62001ae146d454b2ca8c069d1ad7547bb3ce61e538b65a893776d178
fd816c5903c10baf3145dbb4b4af1839c995877ee3eeecf3c5268e9172fca5b3
ef9bc2b680f60772dcd1e9c159018e94ff38d21f9dc651c7c935e5fd7321ac66

Ausgenutzte Schwachstellen
CVE-2013-4979
CVE-2014-8439
CVE-2015-2387
CVE-2015-2419
CVE-2015-2545
CVE-2015-3043
CVE-2015-3105
CVE-2015-5119
CVE-2015-5122
CVE-2015-7645
CVE-2016-1019
CVE-2016-4117
CVE-2017-0199
CVE-2018-0802
CVE-2018-4878