Sicherheitswarnungen

Hier finden Sie Beschreibungen und Erläuterungen zu verschiedenen sicherheitsrelevanten Hinweisen, die uns aus vertrauenswürdigen Quellen auf täglicher Basis zugestellt werden.

Diese Informationen leiten wir als BelWü-CSIRT an diejenigen unserer Kunden weiter, bei denen ein entsprechendes potenzielles Sicherheitsproblem entdeckt wurde.

Weiterführende Informationen erhalten Sie hier:
www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Infektionsbeseitigung/Infektionsbeseitigung_node.html [1]

Liste der Sicherheitswarnungen

Im Folgenden eine Liste der Sicherheitswarnungen, zu denen Sie hier weitere Erklärungen finden. Diese Liste wird von uns immer wieder erweitert und aktualisiert.

- Aktive Teilnahme an DDoS Attacken[2]
- DDoS Angriffe mittels Wordpress Pingback[3]
- DNS-Server mit offenem AXFR[4]
- Elasticsearch-Server[5]
- Geodo[6]
- Gestohlene FTP-Zugangsdaten[7]
- mDNS[8]
- Memcached[9]
- MongoDB[10]
- MS-SQL[11]
- NTP Monlist[12]
- Offene LDAP-Server[13]
- Offene MySQL-Datenbanken mit Standard-Passwort[14]
- Offene NetBIOS-Namensdienste[15]
- Online-Banking-Trojaner[16]
- Open Resolver[17]
- Portmapper[18]
- Ramnit[19]
- Redis[20]
- SCADA[21]
- SMB-Backdoor[22]
- SNMP[23]
- SSDP[24]
- Verwundbare ownCloud/Nextcloud-Instanzen[25]

Links

[1] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Infizierte-Systeme-bereinigen/infizierte-systeme-bereinigen_node.html
[2] https://support.belwue.de/sicherheit/sicherheitswarnungen/aktive-teilnahme-an-ddos-attacken/
[3] https://support.belwue.de/sicherheit/sicherheitswarnungen/ddos-angriffe-mittels-wordpress-pingback/
[4] https://support.belwue.de/sicherheit/sicherheitswarnungen/dns-server-mit-offenem-axfr/
[5] https://support.belwue.de/sicherheit/sicherheitswarnungen/elasticsearch-server/
[6] https://support.belwue.de/sicherheit/sicherheitswarnungen/geodo/
[7] https://support.belwue.de/sicherheit/sicherheitswarnungen/gestohlene-ftp-zugangsdaten/
[8] https://support.belwue.de/sicherheit/sicherheitswarnungen/mdns/
[9] https://support.belwue.de/sicherheit/sicherheitswarnungen/memcached/
[10] https://support.belwue.de/sicherheit/sicherheitswarnungen/mongodb/
[11] https://support.belwue.de/sicherheit/sicherheitswarnungen/ms-sql/
[12] https://support.belwue.de/sicherheit/sicherheitswarnungen/ntp-monlist/
[13] https://support.belwue.de/sicherheit/sicherheitswarnungen/offene-ldap-server/
[14] https://support.belwue.de/sicherheit/sicherheitswarnungen/offene-mysql-datenbanken-mit-standard-passwort/
[15] https://support.belwue.de/sicherheit/sicherheitswarnungen/offene-netbios-namensdienste/
[16] https://support.belwue.de/sicherheit/sicherheitswarnungen/online-banking-trojaner/
[17] https://support.belwue.de/sicherheit/sicherheitswarnungen/open-resolver/
[18] https://support.belwue.de/sicherheit/sicherheitswarnungen/portmapper/
[19] https://support.belwue.de/sicherheit/sicherheitswarnungen/ramnit/
[20] https://support.belwue.de/sicherheit/sicherheitswarnungen/redis/
[21] https://support.belwue.de/sicherheit/sicherheitswarnungen/scada/
[22] https://support.belwue.de/sicherheit/sicherheitswarnungen/smb-backdoor/
[23] https://support.belwue.de/sicherheit/sicherheitswarnungen/snmp/
[24] https://support.belwue.de/sicherheit/sicherheitswarnungen/ssdp/
[25] https://support.belwue.de/sicherheit/sicherheitswarnungen/verwundbare-owncloud-nextcloud-instanzen/

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/