News Archiv

Navigation

30. Halbjahresbericht MELANI zur Problematik von Personendaten im Netz

30.04.2020 - Der 30. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cybervorfällen der zweiten Jahreshälfte 2019 in der Schweiz wie auch international. Schwerpunktthema im aktuellen Bericht bildet der Umgang und die Problematik von Personendaten im Netz.

MELANI-Halbjahresbericht: Cybersicherheitslage während Corona

29.10.2020 - Der 31. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cybervorfällen der ersten Jahreshälfte 2020 in der Schweiz und international. Im aktuellen Bericht wird als Schwerpunktthema die Corona-Pandemie beleuchtet.

Update Verschlüsselungs-Trojaner: Neue Vorgehensweise

30.07.2019 – In den vergangenen Wochen wurden Schweizer Unternehmen Ziel einer neuen Art von Angriffen, mit der unbekannte Angreifer Unternehmensnetzwerke erfolgreich infiltrieren und deren Daten mittels einem Verschlüsselungstrojaner grossflächig verschlüsseln. Auch diverse namhafte Schweizer Unternehmen sind von den Angriffen betroffen.

Verschlüsselungstrojaner greifen vermehrt gezielt Unternehmensnetzwerke an

09.05.2019 - Seit Anfang 2019 häufen sich die Meldungen von KMUs und Grossunternehmen im In- und Ausland, dass deren Daten von Verschlüsselungstrojanern, sogenannter «Ransomware», verschlüsselt und somit unlesbar gemacht wurden. Bei diesen Angriffen wurden teilweise auch die Backups verschlüsselt. Dadurch wird die Wiederherstellung der Geschäftstätigkeit der betroffenen Unternehmen unmöglich.

E-Banking: Angreifer haben es auf Aktivierungsbriefe abgesehen

17.08.2017 - Ende 2016 hat MELANI in einem Newsletter darauf hingewiesen, dass Kriminelle vermehrt mobile Authentifizierungsmethoden beim E-Banking im Visier haben. Nun gehen die Angreifer einen Schritt weiter und versuchen Opfer dazu zu bringen, eine Kopie des von der Bank erhaltenen Briefes, welcher Aktivierungsdaten für die die Zwei-Faktor Authentifizierung (2FA) des E-Bankings enthält, an die Betrüger zu senden.

Kritische Verwundbarkeit in Microsoft Windows Server (SIGRed)

Am vergangenen Dienstag Abend (14. Juli 2020) hat Microsoft ein Sicherheitsupdate für eine kritische Verwundbarkeit im Windows Domain Namen System (winDNS) veröffentlicht. Microsoft stuft die Verwundbarkeit mit 10.0 Punkte im CVSS (Common Vulnerability Scoring System) ein, was dem Maximum auf der verfügbaren Skala entspricht.

Warnung vor gefälschten E-Mails im Namen des BAG

14.03.2020 - Seit Freitagmittag (13. März 2020) versuchen Cyberkriminelle die Verunsicherung der Bevölkerung aufgrund der Situation um das Coronavirus auszunutzen. Anhand von E-Mails mit gefälschtem Absender des BAG versuchen sie, Malware zu verbreiten. Die Melde- und Analysestelle Informationssicherung MELANI warnt die Bevölkerung. Diese E-Mails sind umgehend zu löschen.

Vorsicht: Weiterhin erhöhtes Sicherheitsrisiko durch Ransomware gegen KMUs

19.02.2020 - In den vergangenen Wochen hat MELANI / GovCERT mehr als ein Dutzend Ransomware-Fälle bearbeitet, bei welchen unbekannte Täter die Systeme von Schweizer KMUs und Grossbetrieben verschlüsselt und damit unbrauchbar gemacht haben. Die Angreifer stellten Lösegeldforderungen von mehreren zehntausend Franken, vereinzelt auch von Millionenbeträgen.

Microsoft stellt für ältere Produkte den Support ein: Gefahr droht

Bern, 16.12.2019 - Gemäss einer Mitteilung von Microsoft werden am 14. Januar 2020 für verschiedene ältere Produkte der Support und somit die Updates eingestellt. Betroffen sind folgende Produkte: Betriebssystem «Windows 7», «Windows Server 2008» und «Windows Server 2008 R2».

Verschlüsselungstrojaner weiterhin auf dem Vormarsch

29.10.2019 - Der 29. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cybervorfällen der ersten Jahreshälfte 2019 in der Schweiz wie auch international. Im aktuellen Bericht werden als Schwerpunktthema die Cyberangriffe mit Verschlüsselungstrojanern beleuchtet, welche im ersten Halbjahr 2019 weltweit grossen Schaden angerichtet haben.

Warum das Internet of Things (IoT) einen Strom-Blackout verursachen könnte

IoT-Geräte können in grossem Masse für Cyber-Angriffe missbraucht werden, Erfolgreiche Erpressungsversuche (z.B. «Fake Sextortion») sowie Überweisungsbetrug mit «Office 365»-Zugangsdaten und das Schwergewichtsthema «Umgang mit eingekauften Risiken bei Hard- und Software»: Der am 30. April 2019 veröffentlichte 28. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cyber-Vorfällen der zweiten Jahreshälfte 2018 im In- und Ausland.

Sextortion: Zahlreiche Schweizerinnen und Schweizer betroffen – Behörden lancieren «www.stop-sextortion.ch»

Erpresser behaupten in einer Mail, Zugang zu Computer und Webcam zu haben und drohen damit, Bilder und Videos mit sexuellem Inhalt zu veröffentlichen, sollte kein Lösegeld bezahlt werden. Diese Betrugsmasche wird Fake-Sextortion genannt und dabei wird typischerweise eine Bezahlung in Bitcoins gefordert. Mit dieser Betrugsmethode haben Kriminelle in den letzten sechs Monaten trotz der kleinen geforderten Summen Bitcoins im Wert von ca. 360'000 CHF erbeutet. Solange die betroffenen E-Mail-Empfänger Lösegeld bezahlen, wird dieses Vorgehen befeuert und weiterhin eingesetzt. Helfen Sie mit, diese Masche zu stoppen und zahlen Sie kein Lösegeld. Auf der Webseite www.stop-sextortion.ch, die von den Behörden heute lanciert wurde, finden Sie Informationen und können Fake-Sextortion E-Mails melden.

Trojaner Emotet wieder aktiv

Nach mehrmonatigem Unterbruch beobachtetet MELANI erneut verschiedene Malspam-Wellen mit infiziertem Word-Dokumenten im Anhang. Dabei handelt es sich um einen bereits länger bekannten Trojaner namens Emotet (auch bekannt als Heodo). Ursprünglich als E-Banking-Trojaner bekannt, wird Emotet heute vor allem für den Versand von Spam sowie das Nachladen von weiterer Schadsoftware (Malware) verwendet. Emotet versucht - mit gefälschten E-Mails im Namen von Kollegen, Geschäftspartnern oder Bekannten - mittels Social-Engineering den Empfänger zum Öffnen des Word-Dokuments sowie zum Ausführen der darin enthaltenen Office-Makros zu verleiten.

Wer das gleiche Passwort mehrfach nutzt, hilft den Angreifern

08.11.2018 - Der am 8. November 2018 veröffentlichte 27. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cyber-Vorfällen der ersten Jahreshälfte 2018 im In- und Ausland. Das Schwerpunktthema ist den Lücken in Hardware gewidmet. Im Fokus stehen zudem unter anderem der gezielte Malware-Angriff, für den der Name des Labors Spiez missbraucht worden ist sowie verschiedene Datenabflüsse und die Problematik bei der Mehrfachnutzung eines Passwortes.

Wieder vermehrt betrügerische Anrufe bei Firmen

05.07.2018 - In den letzten Tagen mehren sich wiederum Anrufe bei potenziellen Opferfirmen, in denen sich Angreifer als Bankmitarbeiter ausgeben. Die Anrufer bitten um die Ausführung von Zahlungen oder geben vor, ein Update beim E-Banking durchführen zu müssen, das anschliessend getestet werden soll.

Einkaufskorb

https://www.ncsc.admin.ch/content/ncsc/de/home/aktuell/news/news-archiv.html