SWITCH Security Report zu aktuellen Trends im Bereich IT-Security und Privacy

März/April 2020

I. Ein Virus kommt selten allein – Wie sich mit Corona auch Computerviren pandemisch ausbreiten

Die Corona-Pandemie hat der Schweiz einen noch nie dagewesenen Digitalisierungs- und Remote-Work / Computing-Schub verliehen. Nie zuvor haben so viele Schweizerinnen und Schweizer im Home Office gearbeitet. Was die Ausbreitung des realen, Menschen und ihr Immunsystem angreifenden Virus stoppen oder zumindest verlangsamen soll, fördert die Verbreitung virtueller Viren, die Netzwerke, Server, Computer, Tablets und Smartphones befallen.

Das hat im Wesentlichen sechs Gründe:

1) Die Aufforderung zum Umzug ins Home Office kam für viele Unternehmen wie auch für deren Mitarbeitende überraschend und in vielen Fällen extrem kurzfristig. Viele traf der Zwang zur plötzlichen digitalen Heimarbeit völlig unvorbereitet. Fragen der Cyber Security hatten dabei in den wenigsten Fällen Priorität.

2) Viele Business Devices sind nun wireless oder verkabelt in private Netzwerke eingebunden, deren Sicherheitsstandard nicht dem vieler Unternehmen entspricht.

3) Mühsam erlernte Security-Prozesse (z.B. kein Einstecken fremder USB-Sticks, keine Downloads von Software, die nicht vom IT-Admin geprüft und zugelassen wurde, usw). wurden und werden so schnell vergessen wie der Schnee von gestern.

4) Mit der Dezentralisierung der Devices hat sich die Zahl der involvierten Netzwerke und generell die Angriffsfläche für Cyberkriminelle exponentiell vergrössert.

5) Heimarbeitende bekommen plötzlich Anfragen von Personen, Einladungen zu Online-meetings und Aufforderung zur Übersendung oder Entgegennahme von Daten, die entweder von ihrem Unternehmen oder aber – und dann wird es prekär – von Adressen stammen, die sich als dieses Unternehmen ausgeben. Oft können sie nicht unterscheiden, was echt und was Fake ist.

6) Zuhause wird der Versuchung leichter nachgegeben, Privates auf Firmendevices herunterzuladen.

Eine (für deren Zwecke) derart günstige Gelegenheit lassen sich Cyberkriminelle natürlich nicht entgehen. Bereits am ersten Tag des Lockdowns berichtete die Melde- und Analysestelle Informationssicherung des Bundes (MELANI), dass Betrüger aktuell Erpresser-Mails verschickten. Eine Woche später beklagte MELANI, dass mit dem Coronavirus im Netz betrogen, gefaked und gephisht würde wie nie zuvor. Und noch immer ist das brandgefährliche Erpresser-Software-Trio Emotet/Trickbot/Ryuk unterwegs, um komplette Netze lahmzulegen und Firmen und Organisationen bis an die Grenzen ihrer Belastbarkeit und darüber hinaus zu erpressen. Wovor wir im SWITCH Security Report 6-2019 eindringlich gewarnt hatten, führte bisher in der Schweiz unter anderem dazu, dass der renommierte Fensterhersteller "Swisswindows AG" als Folge einer Ryuk-Attacke Insolvenz hat anmelden müssen.

Das Thema "Cyber Security im Home Office" darf also nicht verdrängt werden, im Gegenteil: Awareness war noch nie so wichtig. Deshalb hat MELANI am 24.03.2020 einen Awareness-Appell an alle Nutzer im Home Office veröffentlicht. Am 02.04.2020 hat MELANI Endbenutzer Guidelines nachgeschoben. Weitere gute Quellen sind wie immer ibarry.ch und die Empfehlungen für’s sichere Home Office von Europol, siehe Links und der nächste Artikel.

Nachzulesen unter:

https://www.melani.admin.ch/melani/de/home.html
https://www.heise.de/newsticker/meldung/Abzocke-im-Onlinehandel-Muehsamer-Kampf-gegen-Corona-Geschaefte-4694227.html
https://www.bleepingcomputer.com/news/security/trickbot-emotet-malware-use-coronavirus-news-to-evade-detection/
https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH-Security-Report-2019-06-de.pdf
https://www.inside-it.ch/de/post/ein-cyber-angriff-hat-uns-in-arge-bedraengnis-gebracht-20200228
https://dataloft.ch/security/schweizer-fensterfirma-swisswindows-ag-geht-nach-ransomware-angriff-pleite
https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/fernzugriff.html
https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/fernzugriff-enduser.html
https://ibarry.ch
https://ibarry.ch/wp-content/uploads/2020/03/safe-at-home_FINAL.pdf

II. Die zehn wichtigsten Regeln fürs sichere Arbeiten im Home Office

Was können Unternehmen und deren Mitarbeitende tun, um Telearbeit im Home Office so sicher zu machen wie möglich? Viele wichtige, grundlegende und nützliche Tipps bietet zum einen die Security Checkliste auf iBarry.ch (iBarry ist der "Bernhardiner", der im Auftrag der Swiss Internet Security Alliance, der auch SWITCH angehört (Link siehe unten), vor den Gefahren des Internets schützt). Zum anderen hat das SANS Institut je einen Guide fürs sichere Arbeiten im Home Office zusammengestellt. Beide sind unter den untenstehenden Links abrufbar. Zum schnellen Überblick haben wir die aktuell wichtigsten Tipps hier zusammen-gestellt:

1) Nutzen Sie für alle Business-Aktivitäten den VPN-Kanal Ihres Unternehmens
2) Trennen Sie Arbeit und Privates so gut es möglich ist: Optimal ist natürlich ein eigener Raum oder ein abgeteilter "Work Space" und ein eigenes Gerät fürs Arbeiten (Desktop, Laptop, Tablet oder Smartphone).
3) Sichern Sie Business-Geräte und -Dokumente vor fremdem Zugriff – je nach Geheimhaltungsstufe auch vor dem Ihrer Mitbewohnerinnen und-bewohner, Kinder oder Lebensgefährten.
4) Bleiben Sie aufmerksam gegenüber fremden Mails, Aufforderungen, an Ihren Geräten oder der Software Änderungen vorzunehmen oder Zusatzprogramm zu laden.
5) Seien Sie vor vermeintlichen "Corona-Specials" auf der Hut, die auch gerne dazu benutzt werden, Ihre Daten abzuphishen oder Ihre Geräte mit Malware zu infizieren.
6) Sichern Sie Ihren Computer oder ihr Gerät mit einem starken Passwort.
7) Verwenden Sie externe Speicher zur Datensicherung (Festplatten, USB-Sticks, o.ä.) und verschlüsseln Sie auch diese.

8) Verschlüsseln Sie alle sensitiven Daten auf Clients.

9) Schützen Sie alle Businessgeräte vor Missbrauch durch eine starke Authentifizierung – z.B. zwei Wege-Authentifizierung via Device und SMS-Code aufs Mobiltelefon.

10) Beachten Sie die Sicherheitsregeln, die in Ihrem Unternehmen gelten, auch zu Hause.

Nachzulesen unter:

https://ibarry.ch/digitale-sicherheit
https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit
https://security-awareness.sans.org/sites/default/files/2020-03/01-SSA-Coronavirus-WorkingFromHome-DeploymentGuide_German_0.pdf
https://security-awareness.sans.org/sites/default/files/2020-03/03-SSA-Coronavirus%20-WorkingFromHome-CheatSheet_German.pdf

III. Online-Meetings – wie sicher sind Cisco WebEx und Zoom?

Software für Online-Meetings ist derzeit gefragt wie nie. Mittlerweile weisen viele Experten aber auch darauf hin, dass zwei der beliebtesten Applikationen zumindest in ihren Gratis- oder Low-Budget-Versionen Probleme mit Privatsphäre und/oder Sicherheitslücken haben.

So behält sich beispielsweise Ciscos Online-Meeting-Service WebEx vor, Daten zu sammeln, zu speichern und an Dritte weiterzugeben. Originalton WebEx: "We may share Registration Information, Host Information, and/or Usage Information with service providers, contractors or other third parties to assist in providing and improving the service."

Zudem wurden in WebEx mehrere Sicherheitslücken entdeckt. Sowohl via WebEx Network Recording Player als auch via Cisco WebEx Spieler könnten Angreifer auf Geräte zugreifen und diese mehr oder weniger umfassend fernbedienen, um beliebigen Code auf dem System des Zielbenutzers auszuführen.

Noch sammelbegeisterter zeigt sich ein anderer sehr beliebter Meeting-Service: Zoom. Die Liste der Daten, die Zoom gemäss der eigenen Datenschutzerklärung sammelt, umfasst mehrere Bildschirmseiten (siehe Link unten). Zudem war auch Zoom bereits Opfer eines grösseren Hacks. Und obendrein berichtet dataloft.ch, dass Investigativ-Journalisten von "The Intercept" herausgefunden haben wollen, dass der Zoom-Aussage, dass die Meetings End-to-End verschlüsselt seien, eine Zoom-eigene Definition von End-to-End-Verschlüsselung zugrunde liege, die es zwar keinen Hackern, wohl aber dem Anbieter theoretisch ermöglicht, auf unverschlüsselte Video- und Audiodaten von Meetings zuzugreifen.

Tatsächlich lassen sich bei genauer Analyse von Zoom einige Probleme bezüglich der Privatsphäre, sowie Bugs finden, die sowohl unter Windows als auch unter Mac-OS gewisse Sicherheitsrisiken bergen. Da Zoom andererseits bestens für grosse Online-Meetings und -Vorlesungen geeignet ist, wollen und können viele dennoch nicht auf den webbasierten Service verzichten. Das müssen sie auch nicht, wenn sie die folgenden sieben Sicherheitshinweise beachten:

1) Entwickeln oder aktualisieren Sie vor dem Einsatz ein Konzept für die Nutzung von Cloud-Services, in dem Sie Themen wie z.B. Datenschutz, Klassifizierung von Daten, welche Daten dürfen in keinem Fall in einer Cloud prozessiert/gespeichert werden, etc. geregelt haben.
2) Halten Sie Ihre Zoom-Applikation auf dem neusten Stand.
3) Kündigen Sie Zoom-Meetings nicht öffentlich (z.B. auf Twitter oder LinkedIn etc.) an.
4) Generieren Sie zufällige Zoom-Meeting IDs.
5) Schützen Sie Ihre Meetings mit einem Passwort.
6) Managen Sie die Teilnahme an Ihren Meetings: Unterdrücken Sie zunächst Mikrofon und Kamera. Richten Sie für die Teilnehmenden einen Warteraum ein. Lassen Sie dann die Teilnehmenden einzeln ins Meeting. Aktivieren Sie "lock", wenn alle Teilnehmer im Meeting sind. Dann deaktivieren Sie Kamera- und Mikro-Unterdrückung und beginnen mit dem Meeting.
7) Benutzen Sie keinesfalls Logins via Facebook oder Google, sondern vergeben Sie dezidierte Username/Passwort-Kombinationen zum Einloggen.

Nachzulesen unter:

https://www.linkedin.com/pulse/using-google-meet-zoom-webex-other-video-conferencing-jeffrey-carr/?published=t
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-cisco-webex-network-recording-player-and-cisco-webex-player-could-allow-for-arbitrary-code-execution_2020-032
https://zoom.us/de-de/privacy.html
https://dataloft.ch/security/end-to-end-verschluesselung-von-zoom-unter-beschuss

IV. Echt jetzt? Ransomware Gangs entwickeln in der Corona-Pandemie eine Art "Ehrencodex"

Zur folgenden Nachricht enthalten wir uns jeden Kommentars. Erwähnenswert finden wir sie allemal. Deshalb überlassen wir die Einordnung unseren geschätzten Leserinnen und Lesern. Die Cyberkriminellen-Organisationen CLOP Ransomware, DoppelPaymer Ransomware, Maze Ransomware, Nefilim Ransomware und Netwalker Ransomware

erklärten einem Bericht von bleepingcomputer.com zufolge, dass sie während der Covid-19-Pandemie Attacken auf Spitäler, medizinische Einrichtungen und andere Gesundheitsorganisationen aussetzen wollten. Gegenüber der Redaktion betonten alle mehr oder weniger unisono, sie würden ohnehin nie bewusst Spitäler angreifen. Wer nun aber auf die läuternde Wirkung des Corona-Virus gehofft hatte, sah sich sogleich wieder enttäuscht. Denn auf Nachfragen, was denn mit den Spitälern geschehe, deren Daten "versehentlich" verschlüsselt worden seien, zeigte ein Vertreter von Netwalker Ransomware dann doch wieder das hässliche Gesicht des Cyberkriminellen: "Wer seine Daten verschlüsselt bekommen hat, muss für die Freigabe zahlen" Punkt.

Nachzulesen unter:

https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/