FEDIL

Publikation

CYBERSECURITY CHECKLIST

Sehr geehrte Damen und Herren,

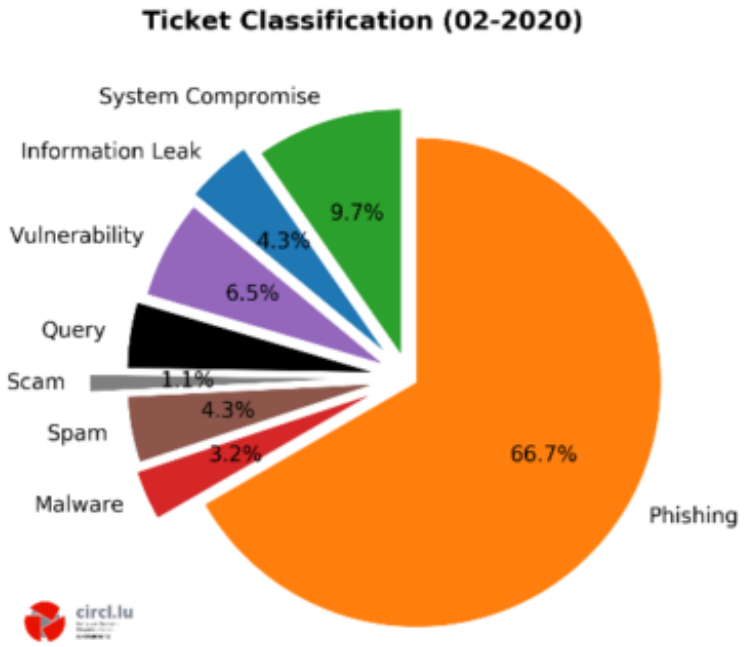
Sehr geehrtes Mitglied,

Die FEDIL möchte Sie in Zusammenarbeit mit SECURITYMADEIN.LU auf bestimmte Elemente der Cybersicherheit aufmerksam machen, die berücksichtigt werden müssen, um die Risiken zu begrenzen und die sich vervielfältigenden und diversifizierenden Cyberangriffe so weit wie möglich zu verhindern.

Es ist immer wichtig, die Cybersicherheit im eigenen Unternehmen genau im Auge zu behalten und für adäquate Massnahmen zu sorgen. Dies ist im Zusammenhang mit der Coronavirus-Krise aufgrund des massiven Rückgriffs auf die Telearbeit, die Angreifern Möglichkeiten eröffnet, wichtiger denn je. Telearbeit fördert die Nutzung von E-Mail für die Kommunikation und schafft damit perfekte Bedingungen für E-Mail-Betrugsschemen.

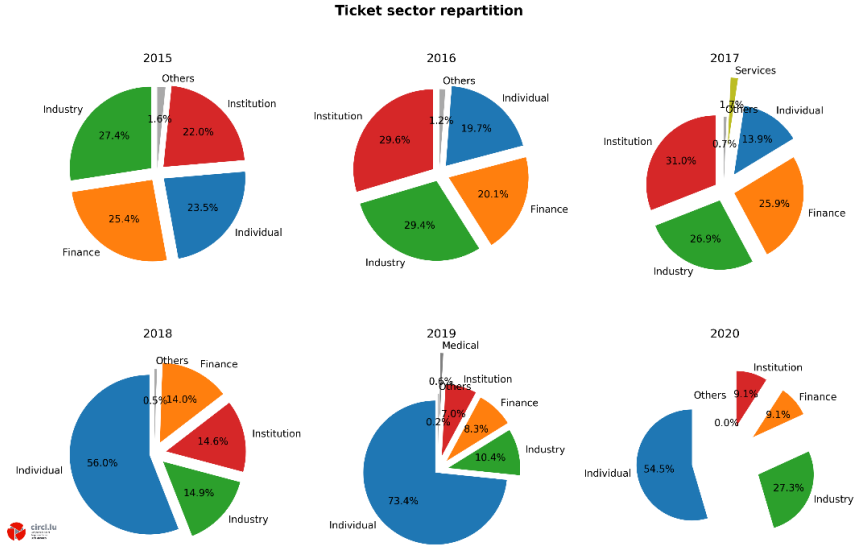
Auch wenn die Zahl der Angriffe nicht wesentlich zunimmt, erlebt eine bestimmte Art von Angriffen in der Tat ein Wiederaufleben, nämlich das Phishing. Die CIRCL-Zahlen vom vergangenen Februar zeigen die Bedeutung solcher Angriffe mit 66,7% (siehe Grafik unten). Genau hier liegt das Problem, denn diese Art von Angriffen nutzt den menschlichen Faktor aus und richtet sich direkt an Benutzer, die oft nicht ausreichend vorbereitet sind, um eine betrügerische E-Mail zu erkennen. Die Motivation für diese Angriffe ist in erster Linie finanzieller Natur. Das Ziel besteht darin, die gegen ein Lösegeld, die berühmte „Lösegeldforderung“, erlangten Informationen zu monetarisieren.

Die jüngsten lokalen Beispiele zielten bisher auf die in der Presse erwähnten Unternehmen Cactus und Tarkett ab. Im Fall von Cactus war die Gruppe das Ziel der Lösegeldforderung von REvil. Die von den Hackern gestohlenen Daten wurden im Internet veröffentlicht, um die Gruppe zur Zahlung des geforderten Lösegeldes zu zwingen.



Es ist daher unerlässlich, die Mitarbeiter des Unternehmens für die Risiken zu sensibilisieren, die durch den Missbrauch der Geräte, schlechtes Verhalten und die Folgen eines Cyberangriffs entstehen können.

Darüber hinaus werden, wie in der Grafik unten dargestellt, alle von IT-Infrastrukturen abhängigen Tätigkeitsbereiche, unabhängig von der Unternehmensgröße, anvisiert.



Folglich erinnert Sie die FEDIL im Folgenden an die von SECURITYMADEIN.LU vorgeschlagenen praktischen Ratschläge:

E-MAILS

– Verwenden Sie geschäftliche E-Mail-Konten anstelle von persönlichen Konten

für arbeitsbezogene E-Mails mit persönlichen Daten. Wenn persönliche E-Mails verwendet werden, stellen Sie sicher, dass der Inhalt und die Anhänge verschlüsselt sind, und vermeiden Sie die Verwendung persönlicher oder vertraulicher Daten in den Betreffzeilen.

– Bevor Sie eine E-Mail versenden, stellen Sie sicher, dass Sie sie an den richtigen Empfänger senden, insbesondere bei E-Mails, die große Mengen an personenbezogenen Daten oder sensiblen persönlichen Daten enthalten.

– Wenn möglich, sollten Sie es vorziehen, jedes Mal verschlüsselte E-Mails zu versenden.

GERÄTE

– Achten Sie besonders darauf, dass Geräte wie USB-Sticks, Telefone, Laptops oder Tablets nicht verloren gehen oder verlegt werden.

– Verwenden Sie vorzugsweise den professionellen Computer. Wenn dies nicht möglich ist, suchen Sie nach Updates, bevor Sie den Heimcomputer benutzen. Richten Sie getrennte Konten für Familienmitglieder ein.

– Stellen Sie sicher, dass jedes Gerät über die erforderlichen Aktualisierungen verfügt, z. B. Betriebssystem-Updates (wie iOS oder Android) und Software-/Virenschutz-Updates.

– Stellen Sie sicher, dass der Computer, Laptop oder das Gerät an einem sicheren Ort verwendet wird, z.B. an einem Ort, an dem man es sehen kann, und minimieren Sie, wer sonst noch den Bildschirm sehen kann (insbesondere wenn die Person mit sensiblen persönlichen Daten arbeitet).

– Sperren Sie das Gerät, wenn es aus irgendeinem Grund unbeaufsichtigt bleiben soll.

– Stellen Sie sicher, dass die Geräte ausgeschaltet, verriegelt oder sorgfältig aufbewahrt werden, wenn sie nicht in Gebrauch sind.

– Sperren Sie die Kamera, wenn sie nicht verwendet wird.

– Verwenden Sie wirksame Zugangskontrollen (wie Multi-Faktor-Authentifizierung und starke Passwörter) und gegebenenfalls Verschlüsselung, um den Zugriff auf die Kamera einzuschränken und das Risiko zu verringern, wenn ein Gerät gestohlen wird oder verloren geht.

– Wenn ein Gerät verloren geht oder gestohlen wird, ergreifen Sie sofort Maßnahmen, um nach Möglichkeit eine ferngesteuerte Speicherlöschung zu gewährleisten.

CLOUD UND NETZZUGANG

- Konfigurieren Sie die Geräte im Vorfeld, indem Sie Tools wie Firewalls und IT-Hygieneregeln einrichten.
- Verwenden Sie ein virtuelles privates Netzwerk (VPN), um eine direkte und sichere Verbindung mit dem internen Netzwerk des Unternehmens zu gewährleisten und den Datentransfer vor böswilligen Handlungen zu schützen.
- Stellen Sie keine Verbindung zu einem öffentlichen Wi-Fi-Netzwerk her, weder unbekannt noch unkontrolliert. Diese Netzwerke werden häufig von böswilligen Akteuren als bevorzugte Angriffsvektoren benutzt, um Unternehmen über ihre Mitarbeiter ins Visier zu nehmen.
    - Verbinden Sie sich mit 3G- oder 4G-Netzen, wenn Sie keinen

Zugang zu einer sicheren Wi-Fi-Verbindung haben.

- Verwenden Sie so weit wie möglich nur die vertrauenswürdigen Netzwerke oder Dienste der Organisation und befolgen Sie alle organisatorischen Regeln und Verfahren bezüglich Cloud- oder Netzwerkzugang, Verbindung und Datenaustausch.
- Wenn Sie ohne Cloud- oder Netzwerkzugang arbeiten, stellen Sie sicher, dass alle lokal gespeicherten Daten ordnungsgemäß und sicher gesichert sind.
- Fernzugriffssoftware (wie z.B. TeamViewer) sollte sehr vorsichtig und nur von autorisierten Mitarbeitern verwendet werden. Es sollte immer aktualisiert und nur dann verwendet werden, wenn es absolut notwendig ist.
- Überprüfen Sie die Zuverlässigkeit von Videokonferenzplattformen. Insbesondere dort, wo Dateien gespeichert werden, wenn sie übertragen werden. Dasselbe gilt für Dateiübertragungsplattformen.

VIDEOKONFERENZ

Der Einsatz von Videokonferenzen birgt auch Risiken. Es gibt hauptsächlich 3 Arten von Risiken:

– Das Hauptrisiko, das es abzudecken gilt, ist der Datenverlust durch passives und unbefugtes Abhören vertraulicher Gespräche.

– Risiken im Zusammenhang mit der Verletzung der Privatsphäre infolge eines Missbrauchs, Konfigurations- oder Softwarefehlern, die z.B. erlauben: die Kontrolle über die Kamera des Organisators ohne sein Wissen zu übernehmen, den Anruf aufzuzeichnen oder die Daten des Benutzerkontos ohne Genehmigung an Dritte zu senden.

– Austausch von Dokumenten, Präsentationen, Notizen und anderen Chat-Nachrichten (zusätzlich zur Sprache), die sensible Informationen enthalten und auf unkontrollierten Servern landen können.

Wir laden Sie ein, den Empfehlungen von SECURITYMADEIN.LU zu folgen, um die Risiken unter dem folgenden Link zu begrenzen: VIDEOKONFERENZEN UND CYBERSICHERHEIT: WIE LASSEN SICH DIE RISIKEN BEGRENZEN?

Darüber hinaus ist anzumerken, dass die Angreifer versuchen, die Coronavirus-Krise auszunutzen, indem sie sich die durch COVID-19 erzeugte Angst und Unsicherheit zunutze machen. Nachstehend finden Sie eine nicht erschöpfende Liste von Fällen, mit denen Sie möglicherweise konfrontiert werden.

1. Coronavirus-Websites: Einige Angreifer entwerfen Coronavirus-bezogene Websites, um Sie zum Herunterladen einer Anwendung einzuladen, die Sie über die Situation auf dem Laufenden hält. Aber das ist eine Falle!
2. Sicherheitsmassnahmen gegen Coronavirus: Sie sind eingeladen, ein pdf mit Tipps zum Schutz vor dem Virus herunterzuladen. Aber die pdf-Datei enthält bösartigen Code...
3. Gefälschtes Antivirenprogramm gegen Coronavirus: Wenn Sie es installieren, erzeugt es Hintertüren auf Ihrem Computer.
4. Nachahmer, die sich als das Rote Kreuz ausgeben, verkaufen COVID-19-Tests zu Hause.
5. Eine gefälschte Nachricht von der WHO (Weltgesundheitsorganisation) installiert Spyware auf Ihrem Computer.
6. Erpressung durch E-Mails, die Sie mit einem Coronavirus zu infizieren drohen.
7. Telefonscherze von der CDC, in denen die Leute aufgefordert werden, die COVID-19-Impfstoffe zu reservieren.

8. Betrüger, die 1.000-Dollar-Schecks als Wirtschaftshilfe für den Fall einer Pandemie versprechen.
9. Verschiedene „Bleiben Sie sicher vor Coronavirus"-Betrügereien.
10. COVID-19-Reduktionscodes zum Verkauf von Malware und gefälschten Produkten.
11. Sofortige Kommunikationsplattformen sind die Hauptziele von Cyberkriminellen.
12. In diesem Zusammenhang ist auch die Zahl der gefälschten Nachrichten im Steigen begriffen.

Abschließend möchten wir das Auftreten eines weiteren Phänomens hervorheben, das dem Arbeitnehmer den Zugang zum Unternehmensnetzwerk ermöglicht, dessen Auswirkungen jedoch schwer zu erkennen sind. Das ist die Nutzung der Privatsphäre und das Versenden von Erpressungs-E-Mails mit dem Betreff „Ich kenne Ihr Passwort". Der Angreifer behauptet, kompromittierende Informationen über die Person zu haben und verlangt die Zahlung eines Lösegeldes. Wir empfehlen Ihnen dringend, Ihre Mitarbeiter auf diese Art von Angriffen aufmerksam zu machen und sie aufzufordern, die Empfehlungen von SECURITYMADEIN.LU zu befolgen:
https://securitymadein.lu/news/sextortion-scam-e-mails-i-know-your-password/SEXTORSIONS-BETRUGS-E-MAILS: „ICH KENNE IHR PASSWORT".

Ob Coronavirus-Krise oder nicht, es ist wichtig, bei der Konsultation von E-Mails und Websites mit äußerster Vorsicht vorzugehen, und im Zweifelsfall wird dringend empfohlen, die IT-Abteilung und Cybersicherheitsspezialisten zu konsultieren und zu alarmieren.