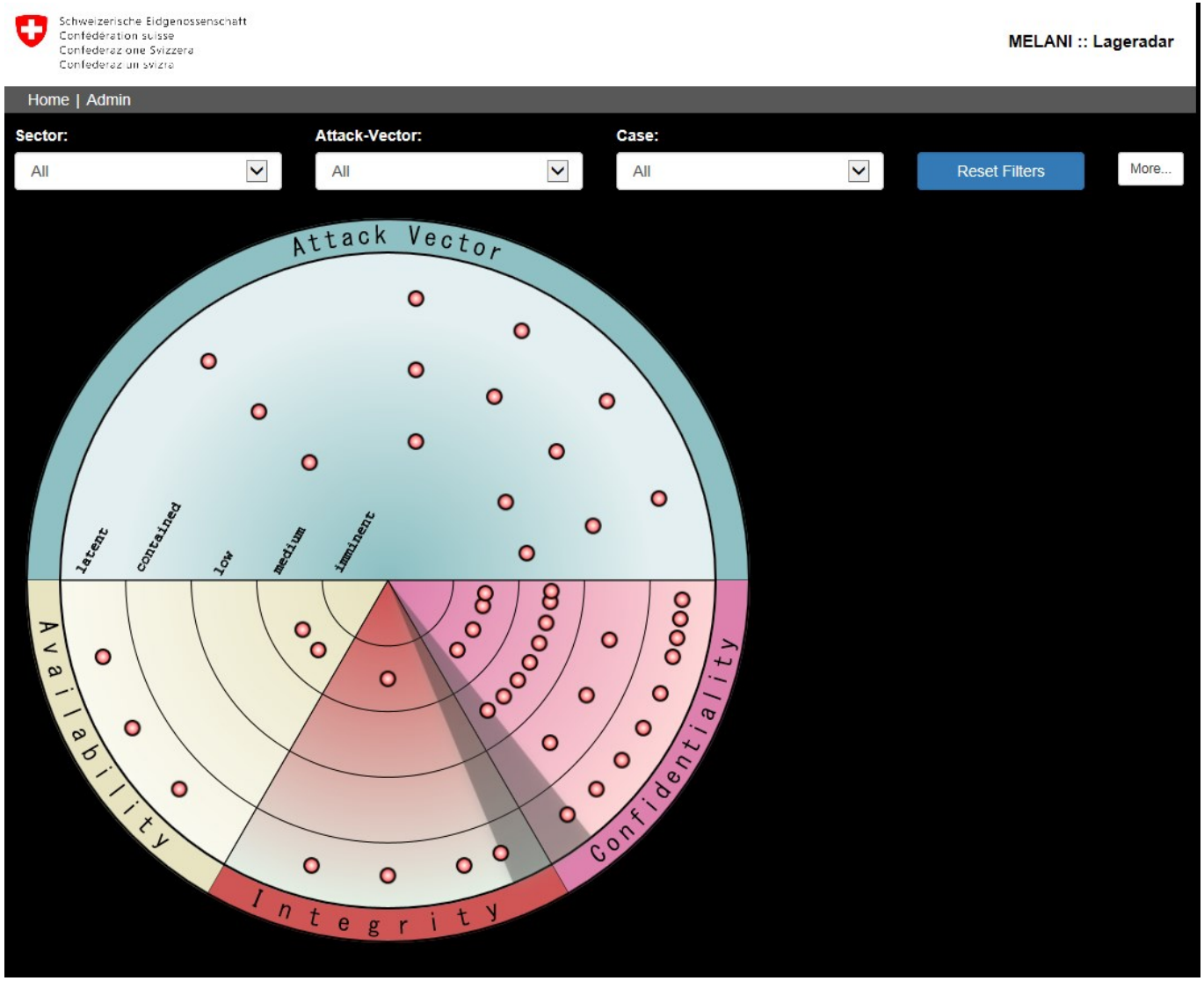
Wahlen und Sicherheit im Netz

13. Juni 2019

Marc Henauer

Die Bedrohungslage Heute



Der Einfache Weg

Und der meistgenutzte Weg

Opfer

Internet

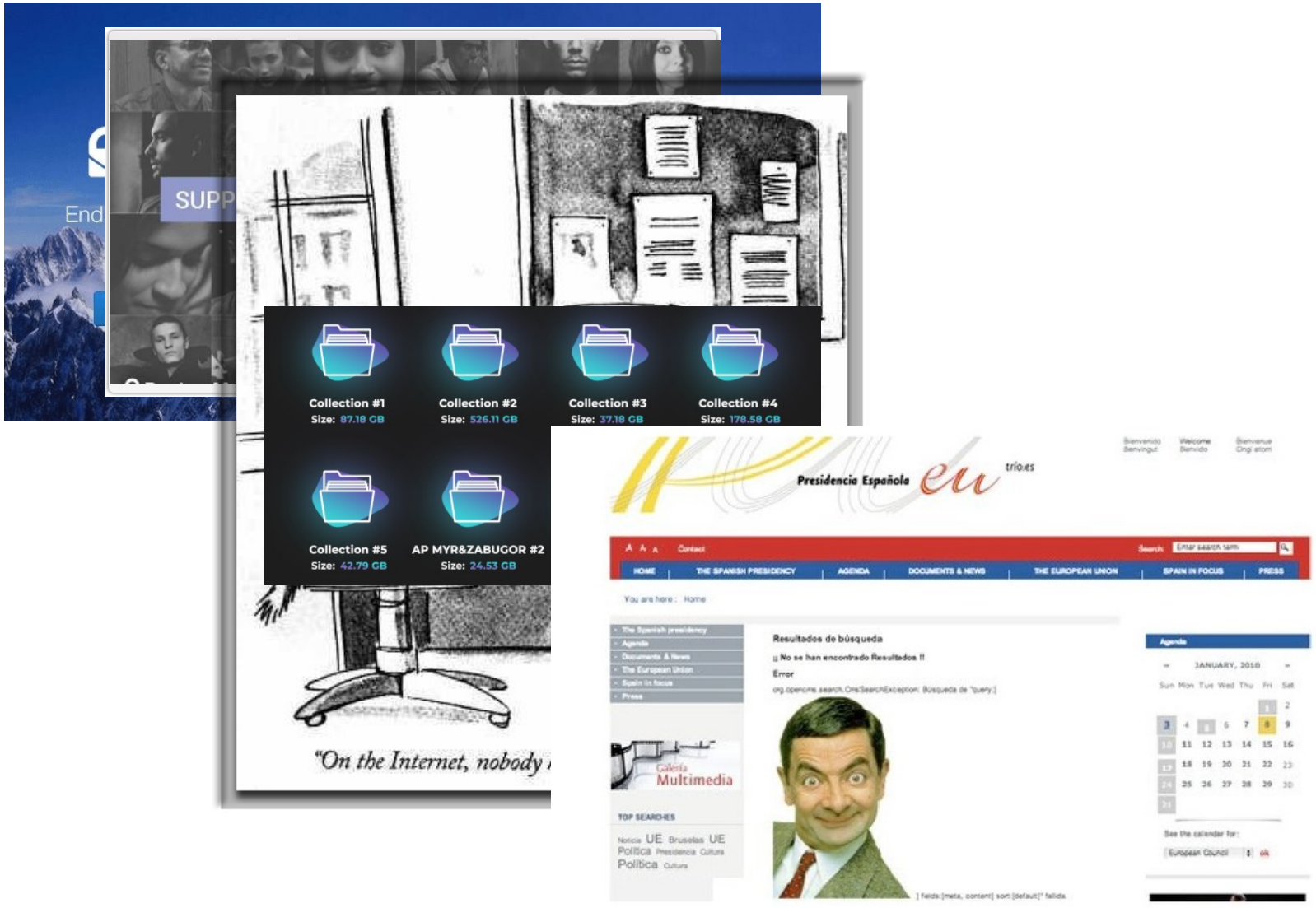
Krimineller

Auch ein Krimineller

Einmal infiziert ist alles möglich

- Der Angreifer hat alle Möglichkeiten des eigentlichen Benutzers.
- Zugriffe auf die gleichen Daten und Files, egal ob lokal oder auf Netzwerken.
- Er besitzt dabei auch die gleichen E-Mail-Kontakte, Benutzernamen, Passwörter und Kreditkartennummern.
- Und noch vieles mehr...

Ausgewählte Beispiele



Schlussfolgerungen

Gefährliche E-Mails: Checkliste für Parlamentarierinnen und Parlamentarier

Die politischen Institutionen und auch Parlamentarierinnen und Parlamentarier geraten zunehmend ins Visier von Cyber-Angriffen. Die jüngsten Fälle, die diesen Trend bestätigen, betrafen zum Beispiel den nationalen Partei-Vorsitz der US-Demokraten und den deutschen Bundestag. Zugang zu den Systemen verschaffen sich die Cyberpiraten sehr oft mit Hilfe von betrügerischen E-Mails, in denen sie die Adressaten auffordern, vertrauliche Informationen zu übermitteln oder einen Link anzuklicken respektive einen Anhang zu öffnen, welcher eine Schadsoftware beinhaltet. Durch Befolgen einiger einfacher Regeln kann man sich relativ gut gegen solche Angriffe schützen.

1. Phishing- und andere betrügerische E-Mails erkennen

Beim Phishing versuchen die Cyberpiraten, die Benutzer/innen dazu zu bringen, vertrauliche Daten preiszugeben (z. B. die Zugangsdaten ihrer E-Mail-Konten oder weiterer Onlinedienste). In einem solchen E-Mail wird den Adressaten zum Beispiel vorgegaukelt, ihre Kontoinformationen seien nicht mehr sicher oder nicht mehr aktuell und müssten über einen entsprechenden Link im E-Mail geändert oder verifiziert werden. Der Link führt dann allerdings nicht auf die Originalseite des E-Mail-Providers oder Social Media Anbieters, sondern auf eine identisch gestaltete und vom Betrüger aufgesetzte Webseite, über welche er die Zugangsdaten dann abfischt.

Eine zweite, oft verwendete Methode besteht im Versand eines E-Mails mit einem Link oder einem Anhang, die dazu dienen, eine Schadsoftware auf dem Computer der Benutzer/innen zu installieren. Die Betrüger haben zahlreiche Tricks, um ihre Opfer zu täuschen und sie im Glauben zu wähnen, es handle sich um legitime E-Mails. Der Absender ist jedoch gefälscht und es wird ein plausibles Szenario präsentiert, um die Adressaten zum Anklicken eines Links oder zum Öffnen eines Anhangs zu verleiten.

2. Risikobewusstsein schärfen

Haben die Benutzer/innen ihre Zugangsdaten im Rahmen eines Phishing-Angriffs preisgegeben, können sich die Cyberpiraten vollen Zugriff auf das Konto der Opfer verschaffen. Sie können im Konto gespeicherte Daten herunterladen oder betrügerische Mails an die Kontakte der Opfer versenden, indem sie sich hinter deren Identität verbergen. Ist es den Piraten gelungen, eine Schadsoftware zu installieren, haben sie grundsätzlich vollumfänglichen Zugang: Sie können den Computer des Opfers ganz nach Belieben fernsteuern, auf alle Konten zugreifen und jegliche Daten einsehen.

./.

3. Sich gegen betrügerische E-Mails schützen

Als Erstes empfiehlt sich generell eine gesunde Portion Misstrauen gegenüber E-Mails. Lieber ein E-Mail ungelesen löschen und nur diejenigen öffnen, bei denen Sie sich absolut sicher sind, dass der Betreff stimmt und der Absender authentisch ist. Im Zweifelsfalle lohnt es sich, wenn möglich, über einen bereits etablierten Zweitkanal (bspw. bekannte Telefonnummer) rückzufragen. Insbesondere empfiehlt MELANI:

- Allen E-Mails zu misstrauen, die unerwartet eintreffen, vor allem wenn Sie darin aufgefordert werden, einem Link zu folgen oder einen Anhang zu öffnen.
- Öffnen Sie in einem verdächtigen E-Mail niemals die Anhänge, folgen Sie in verdächtigen Nachrichten niemals einem Link und geben Sie niemals persönliche Informationen (Passwort, etc.) preis!
- Aktivieren Sie die Mehrfach-Authentifizierung sowohl für den E-Mail-Verkehr wie auch für Ihre Social Media Konten.
- Verwenden Sie für jedes Online-Konto ein anderes Passwort.

4. Schadensbegrenzung

MELANI empfiehlt allgemein:

- Mitteilungen, welche die berufliche Tätigkeit betreffen, sollten nie über private E-Mail-Konten abgewickelt werden.
- Sensible Mitteilungen sollten durch eine Verschlüsselung geschützt werden.

Empfehlungen, wenn Sie glauben, Opfer eines betrügerischen E-Mails geworden zu sein:

- Ändern Sie die Passwörter aller Onlinedienste, zu denen sich der Cyberpirat Zugang verschafft haben könnte.
- Wenn Sie den Verdacht hegen, Ihr Computer sei infiziert, installieren Sie das Betriebssystem neu und ändern Sie alle Passwörter.

Auf der MELANI-Webseite finden Sie zahlreiche weitere nützliche Informationen: www.melani.admin.ch.

Melden Sie alle verdächtigen E-Mails der Melde- und Analysestelle Informationssicherung (MELANI) an folgende E-Mailadresse: reply@melani.admin.ch.

Fragen?