Malwarebefall – was tun?
Checkliste für Technikbeauftragte angegriffener Unternehmen

Allgemeine flankierende Prozesse

Als geschädigtes Unternehmen sollten Sie bei all den nachstehend beschriebenen technisch-taktischen Massnahmen im Auge behalten, dass gegebenenfalls unter anderem Geschäfts- und Kundenverantwortliche so informiert werden müssen, dass sie ihrerseits kommunizieren können. Zur eigenen Entlastung empfiehlt es sich, die Unternehmenskommunikation einzubeziehen – sie kann auch umgebende Stakeholder identifizieren und eine Priorisierung vorschlagen.

1. Kontaktieren Sie Ihr kantonales Polizeikorps sowie MELANI und definieren Sie zusammen das weitere Vorgehen

> Informieren Sie Ihr kantonales Polizeikorps und MELANI und besprechen Sie, ob die Malware zunächst beobachtet werden soll oder ob Gegenmassnahmen ergriffen werden sollen. Der Entscheid über das weitere Vorgehen hängt wesentlich (aber nicht nur) davon ab, ob ein Geschädigter / eine Geschädigte mit der Täterschaft in Kontakt steht und ob die Täterschaft eine Antwort erwartet. Die Polizei berät im weiteren Vorgehen; insbesondere in Bezug auf die Kommunikation mit der Täterschaft und das Verhalten dieser gegenüber.
> Besprechen Sie, ob ein unmittelbares Ausrücken der Polizei zur Unterstützung sinnvoll ist.

2. Ergreifen Sie Gegenmassnahmen im Firmennetz

> Detektieren Sie täterische URL und IP-Adressen sowie das Ausmass der Infektion.
    > Täterische Links (URL und IP-Adressen) müssen detektiert und umgehend auf dem internen Proxyserver bzw. auf der Firewall blockiert werden. Damit wird eine ungewollte Verbindung zum täterischen Server verhindert.
    > Bei Infektion per E-Mail können gewisse täterische Links (URL und IP-Adresse) unter Umständen relativ einfach entweder direkt im E-Mail (Hyperlink) oder in einem entsprechenden Anhang ausgelesen werden.
    > Anhand der Logs von E-Mail-Server, Proxyserver und Firewall sowie anhand allfälliger weiterer Sicherheitssoftware im Netz des geschädigten Unternehmens kann das Ausmass der Infektion festgestellt und es können die täterischen URL und IP-Adressen detektiert werden.
> Blockieren Sie täterische URL und IP-Adressen auf dem internen Proxyserver bzw. auf der Firewall.
> Trennen Sie möglichst umgehend betroffene Geräte und Computer vom Netzwerk. Aber: Solange die Malware nicht durch die kantonalen Strafverfolgungsbehörden und MELANI oder den Geschädigten / die Geschädigte analysiert worden ist, sollten die infizierten Computer und Geräte durch Letztere nicht ausgeschaltet und stattdessen aufbewahrt werden.

3. Sichern Sie die relevanten Daten

> Sichern Sie die Logdateien und übermitteln Sie diese und die nachfolgenden relevanten Daten zur Ermittlung der Täterschaft an die Strafverfolgungsbehörden:
  > Logs der Proxyserver bzw. der Firewall mit den täterischen URL und IP-Adressen können den Strafverfolgungsbehörden per E-Mail-Anhang übermittelt werden.
  > Wenn die Malware das geschädigte Unternehmen per E-Mail erreichte, soll das E-Mail samt Anhang in eine ZIP-Datei verpackt und den Strafverfolgungsbehörden anschliessend per E-Mail-Anhang zugeschickt werden.
  > Wenn die Malwareinfektion per «drive-by download» erfolgte, soll die Malware wenn möglich durch den Geschädigten / die Geschädigte isoliert, in eine ZIP-Datei verpackt und den Strafverfolgungsbehörden anschliessend per E-Mail-Anhang zugeschickt werden.
  > Wenn die Malwareinfektion per USB-Datenträger erfolgte, soll dieser den Strafverfolgungsbehörden zur Verfügung gestellt werden (Posteinschreiben oder persönliche Übergabe).
  > Allfällige durch den Geschädigten / die Geschädigte selbst vorgenommene Schadsoftware-Analysen können den Strafverfolgungsbehörden per E-Mail-Anhang übermittelt werden.

In Zusammenarbeit mit MELANI und Swiss Cyber Experts