sern, haben sich nun verschiedenste vielversprechende Ansätze hervorgetan, um die Überdiagnostik, namentlich unnötige Prostatabiopsien und eventuell daraus resultierende unnötige invasive Therapien, zu reduzieren. Prostatavolumen, Ergebnisse der digital-rektalen Untersuchung, Alter des Patienten und Familienanamnese wurden bezüglich Prostatakarzinom als unabhängige Risikofaktoren identifiziert und werden längst in diversen Risikokalkulatoren zur verfeinerten Risikostratifizierung eingesetzt.
Basierend auf den Schweizer Daten der ERSPC-Studie wurde neuerdings die Aarau-Prostate-Check-App veröffentlicht. Die signifikant bessere Vorhersagegenauigkeit der App wurde durch eine unabhängige externe Validierung bestätigt [8].
Viele Teilnehmer der Screening-Studien wiesen einen PSA-Wert unterhalb von 3 µg/l auf. Anhand der starken Aussagekraft eines Baseline-PSA-Wertes bei Männern ab 45 Jahren können in diesem Fall die PSA-Verlaufskontrollen in einem sicheren Masse angepasst werden, um die Kosten zu senken und den Patientenkomfort zu erhöhen. Jenen Patienten kann, ebenfalls abhängig von der jeweiligen Risikokonstellation, ein individuelles PSA-Verlaufskontrollintervall von bis zu 8 Jahren angeboten werden [9].
Diese App ist Primärversorgern sowie Urologen über den Appstore bzw. Google-Play zugänglich.

Korrespondenz:
maciej.kwiatkowski@ksa.ch

Referenzen und Tabelle

Online unter: www.sulm.ch/d/pipette → Aktuelle Ausgabe (Nr. 6-2017).

Angelika Bischof, Nick Wenger[1]

Cyber-Risiken im Bereich der Laboratorien

Die zunehmende Digitalisierung von Informationen und die steigende Vernetzung von Systemen machen auch vor den Laboren nicht Halt. Eine Welt ohne Zugang zu elektronisch verfügbaren Informationsplattformen oder ohne die Möglichkeit, rund um die Uhr Informationen und Daten auszutauschen, ist kaum mehr vorstellbar. Mit der steigenden Komplexität erhöhen sich jedoch auch die Risiken gegenüber Beeinträchtigungen und Manipulationen von Systemen, Geräten und Daten, welche im Laborbereich verwendet werden. Es ist daher essentiell, dass sich die Labor-Mitarbeitenden aller Stufen und Bereiche der Risiken, welche sich aus der Nutzung dieser Technologien ergeben, bewusst sind.

Worum geht es?

Im Cyber-Raum lauern viele unsichtbare Gefahren; so zum Beispiel in Form von Cyber-Angriffen. Unter einem Cyber-Angriff versteht man eine beabsichtigte Handlung einer Person oder einer Gruppierung mit der Absicht, die Integrität, Vertraulichkeit oder Verfügbarkeit von Daten, Informationen, Anwendungen oder Systemen zu beeinträchtigen, oder mit dem Ziel, Informationen zu stehlen. Ausprägung und Art von Cyber-Angriffen sind stark abhängig von der Motivation der Täterschaft, aber auch davon, ob es sich um Einzelpersonen, Gruppen oder staatliche Organisationen handelt. Attacken aus dem Cyber-Raum unterscheiden sich von traditionellen Angriffen darin, dass sich die Täter nicht mehr physisch vor Ort befinden müssen, sondern von überall her operieren können. Meist werden zudem sogenannte Verschleierungstechniken angewendet, so dass es zunehmend schwierig wird, allfällige Spuren zurückzuverfolgen. Im Laborbereich kommen verschiedene Motive für Cyber-Angriffe in Frage. Dazu gehört beispielsweise die Absicht, die IT-Systeme von Laboratorien so zu beeinträchtigen, dass die betroffenen Einrichtungen ihre Leistungen nicht mehr vollumfänglich erbringen können. Ebenfalls denkbar sind Cyber-Attacken mit dem Ziel, Analyseergebnisse zu verändern. Geschieht dies beispielsweise bei Laborproben von Patienten, kann dies zu Fehldiagnosen und als Folge davon zur Anwendung von falschen Behandlungsmethoden führen. Ein weiteres Motiv für einen Cyber-Angriff auf ein Labor kann aber auch das Ausspähen von sensitiven Informationen sein, mit dem Ziel, diese missbräuchlich weiterzuverwenden.

Welche Gefahren lauern im Cyber-Raum?

Nachfolgend werden einige der aktuellen Angriffsmethoden sowie mögliche Verhaltensregeln, wie man sich schützen kann, beschrieben.

Social Engineering

Social Engineering bezeichnet die zwischenmenschliche Beeinflussung von Personen mit dem Ziel, bestimmte Verhaltensweisen hervorzurufen und sie damit zur Preisgabe von vertraulichen Informationen oder zu bestimmten Aktionen zu bewegen. So kann ein Angreifer beispielsweise mittels Social Engineering die Hilfsbereitschaft oder Gutgläubigkeit eines Labor-Mitarbeitenden ausnutzen, um an dessen Zugangsdaten für das Laborsystem zu gelangen.

> Denkbar sind Cyber-Attacken mit dem Ziel, Analyseergebnisse zu verändern.

Phishing

Beim Phishing werden fingierte E-Mails mit gefälschten Absenderadressen von bekannten Personen oder Unternehmen und mit vertrauenserweckender Aufmachung versendet. Mittels eines gefälschten E-Mails kön-

1 Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Bevölkerungsschutz BABS, Bern

nen die Betrüger an vertrauliche Daten von ahnungslosen Labor-Mitarbeitenden gelangen. Je nachdem, welche Funktion das Opfer innehat und über welche Berechtigungen es verfügt, kann es sich dabei um die Zugangsdaten von deren E-Mail-Konten, von Laborgeräten oder von ganzen Labornetzwerken handeln.

Schadsoftware in E-Mails

E-Mails sind die am häufigsten eingesetzten Mittel zur Verbreitung von Schadsoftware mit dem Ziel, bösartige Programme auf dem Computer des Mail-Empfängers zu installieren. Öffnet beispielsweise ein Labor-Mitarbeiter oder eine Labor-Mitarbeiterin einen mit einem Schadcode versehenen Anhang, kann dies dazu führen, dass sich die Schadsoftware auf dem entsprechenden Computer, aber auch auf sämtlichen Systemen und Geräten verteilt, welche mit diesem Computer verbunden sind. Das Ziel eines solchen Angriffs kann beispielsweise das Ausspionieren von Passwörtern oder aber Erpressung sein. Bei Letzterem verlangt der Angreifer in der Regel Geld, damit der Schadcode entfernt wird und die Systeme und Geräte wieder zur Verfügung stehen.

DDoS-Attacken

Unter einer DDoS-Attacke (Distributed Denial of Service = Angriff auf die Verfügbarkeit von Online-Diensten) versteht man einen Angriff auf Computer-Systeme mit dem Ziel, deren Verfügbarkeit zu stören. Die Motivation hinter solchen DDoS-Attacken können Erpressung, Schädigung eines Konkurrenten oder politischer Aktivismus sein. So kann beispielsweise ein DDoS-Angriff auf ein Labor einerseits zu materiellen Schäden, aber auch zu Reputationsverlusten führen; insbesondere, wenn nebst der Website auch noch die Online-Systeme zur Übermittlung von Laborbefunden nicht zur Verfügung stehen.

Allgemeine Verhaltensanweisungen

Zu den **organisatorischen** Massnahmen gehören beispielsweise Vorkehrungen, welche im Vorfeld vorbereitet und beim Eintreten eines Ereignisses aktiviert werden. Hierzu gehören z.B. die Umsetzung von Business-Continuity-Management(BCM)-Massnahmen oder der Aufbau eines adäquaten Krisenmanagements.

Im Bereich der **technischen** Massnahmen ist es wichtig, die Sicherheit von Systemen und Geräten (Computer, Analysegeräte, Laborsysteme etc.), welche in Laboratorien eingesetzt werden und mit dem Internet verbunden sind, sicherzustellen. Dazu gehören beispielsweise die Installation einer persönlichen Firewall, die Durchführung von regelmässigen Software-Updates oder die Nutzung von Antiviren-Software etc.

Zusätzlich ist aber auch das **Verhalten jedes einzelnen Benutzers** (Labor-MitarbeiterIn, Labor-LeiterIn, Sicherheitsverantwortliche/r, IT-MitarbeiterIn etc.) von entscheidender Bedeutung. Es ist essentiell, sichere Passwörter zu verwenden, sorgsam mit E-Mails umzugehen und sich achtsam im Internet zu bewegen.

Die **Melde- und Analysestelle Informationssicherung MELANI** empfiehlt bei einem Cyber-Angriff zudem, bei der zuständigen Kantonspolizei eine Strafanzeige gegen Unbekannt einzureichen.

Korrespondenz:
ski@babs.admin.ch

Weitere Informationen

- Weiterführende Informationen zum Thema Cyber sowie zu aktuellen Gefahren im Cyber-Bereich stehen auf der Website der Melde- und Analysestelle Informationssicherung MELANI (www.melani.admin.ch) zur Verfügung.
- 2012 hat der Bundesrat die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» verabschiedet. Informationen hierzu finden Sie unter www.isb.admin.ch.
- Informationen zum Schutz kritischer Infrastrukturen (SKI) sind auf der gleichnamigen Website des Bundesamtes für Bevölkerungsschutz BABS unter www.infraprotection.ch verfügbar.

Verhaltensregeln gegenüber Social Engineering

- Publizieren Sie im Internet nur so viele Informationen wie nötig. Dies gilt besonders für die Publikation der Namen und Funktion von Labor-Mitarbeitenden.
- Seien Sie zurückhaltend mit der Herausgabe von sensitiven Informationen.
- Geben Sie keine vertraulichen Informationen (z.B. Benutzername, Passwort usw.) an Personen weiter. Falls jemand darauf besteht, so melden Sie dies umgehend Ihrem Vorgesetzten, dem Systemverantwortlichen oder dem Dienstleistungsanbieter (sofern die IT nicht selber betrieben wird).

Verhaltensregeln bei Phishing, Schadsoftware in E-Mails und ähnlichen Angriffsmethoden

- Seien Sie vorsichtig, wenn Sie unaufgeforderte E-Mails bekommen. Insbesondere, wenn eine Aktion von Ihnen verlangt und mit Konsequenzen (Geldverlust, Strafanzeige, Konto- oder Kartensperrung, verpasste Chance, Unglück) bei Nichtbeachtung gedroht wird. Besonders vertrauenswürdige Firmen werden gerne als gefälschte Absenderadressen missbraucht.
- Klicken Sie in verdächtigen E-Mails auf keine Anhänge und folgen Sie keinen Links.
- Empfohlen wird, dass solche E-Mails bereits seitens IT herausgefiltert werden und gar nicht erst in die persönlichen Mailboxen der Benutzer gelangen.

Verhaltensregeln bei einer DDoS-Attacke

- Grundsätzlich ist es wichtig, dass sich die IT-Verantwortlichen von Laboratorien bereits im Vorfeld mit dieser Angriffsmethode auseinandersetzen und Massnahmen zur Vorbeugung respektive Abwehrbereitschaft umgesetzt haben. Wichtig in diesem Zusammenhang ist es, die geschäftskritischen Systeme zu identifizieren und entsprechend zu schützen.
- Weitere Informationen erhalten Sie unter www.melani.admin.ch > Dokumentation > Checklisten und Anleitungen