PANIK, WUT, SCHULDGEFÜHLE

Die gefühlten Phasen eines Cyberangriffs

Von Mark Peters, BSI-Digitaler Ersthelfer

INTENSIVE SITUATIONEN WIE EIN ERFOLGREICHER CYBERANGRIFF ERFORDERN VON ALLEN BETEILIGTEN RUHE UND KONZENTRATION. DOCH DAS IST LEICHTER GESAGT ALS GETAN.

Nach der Cyberattacke kommt häufig die Panikattacke. Diese Strategien helfen Ihnen, besser mit den Emotionen nach einem Sicherheitsvorfall umzugehen.

Es passiert in der Regel an einem Freitagnachmittag gegen 15 oder 17 Uhr: Mark Peters, BSI-Digitaler Ersthelfer von Praxismanagement Bublitz-Peters erhält einen Notfallanruf, dass etwas Verdächtiges am Praxisrechner vor sich geht - und die Vorstufe des Wochenendes wird zur Vorhölle.

Cybercrime und andere IT-Sicherheitsvorfälle strapazieren die Nerven aller Beteiligten - von den Praxisteams, die versuchen, das Problem zu beheben, bis hin zu den eingeschalteten IT´lern, dem ZAC (Polizei) und ggf. die Datenschutzbehörde. Das kann ein breites Spektrum von Gefühlen auslösen:

- Selbstverleugnung (speziell im Anfangsstadium)
- Panik
- Wut
- Angst
- Schuldgefühle

Diese Emotionen gehen nicht selten einher mit körperlichen Nebenerscheinungen wie einer erhöhten Herzfrequenz, Schweißausbrüchen, Zittern, Übelkeit und langfristig auch psychischen Problemen; ich habe schon mit Arzthelferinnen gearbeitet, die damit nicht zurechtkamen und einfach gegangen sind.
„Diese Emotionen können sich wie ein Virus in der gesamten Praxis ausbreiten", meint Dr. Patrick Stacey, der eine Studie über die emotionalen Reaktionen und Bewältigungsstrategien von Mitarbeitern während eines Cyberangriffs veröffentlicht hat.
Wenn sich der Stress aufbaut, neigen Führungskräfte und Praxismitarbeiter/innen dazu, nervös zu werden - und anschließend Druck auf Technologieexperten auszuüben, damit das Problem schnell gelöst wird. Doch diese Art von Druck ist nie hilfreich, denn als BSI-Digitaler Ersthelfer suche ich mit allen Beteiligten sichere und schnelle Lösungen.

Dabei kann die Art und Weise, wie ein Unternehmen mit einem Cybersicherheitsvorfall umgeht, über sein Schicksal entscheiden. Technologieexperten und die Praxisleitung müssen also die richtigen Entscheidungen treffen. Ruhe und Besonnenheit sind allerdings nicht nur während

Praxismanagement
Bublitz-Peters GmbH & Co. KG
Rohrbacher Str. 28
69115 Heidelberg

Sitz: Heidelberg
Geschäftsführerin: Silke Bublitz-Peters
Registernummer: HRA 701358
Amtsgericht: Mannheim

Telefon: +49 (0)6221-43 85 00
Telefax: +49 (0)6221-43 85 01 10
Mail: praxischeck@bublitz-peters.de
www.bublitzpeters.de

einer Krise wichtig, sondern bereits im Vorfeld, denn die Emotionskette kann schon viel früher beginnen.

Frust schon vor dem Cyberangriff

Für Security-Profis und Cyberschutzbeauftragten in den Praxen ist es keine Seltenheit, dass sie sich wie Sisyphos vorkommen: In vielen Fällen stellt es bereits eine unüberwindbare Hürde dar, die Mitarbeiter dazu zu bringen, grundlegende Regel, etwa für sichere Passwörter, zu befolgen. Doch Probleme dieser Art beschränken sich nicht nur auf die Mitarbeiter: auch die Praxisleitungen sind teilweise schwer von der Bedeutung der Cybersicherheit zu überzeugen. Im Rahmen einer aktuellen Umfrage von Praxismanagement Bublitz-Peters gaben 95 Prozent der befragten Praxisleitungen an, dass ihnen die finanziellen Mittel, Zeit und Personal fehlen, um Cyberberatung in Anspruch zu nehmen und die erforderlichen IT-Sicherheitsrichtlinien (§75 b SGB V) dokumentiert und nachweislich umzusetzen. Weitere 35 Prozent zeigten sich davon überzeugt, dass erst ein erfolgreicher Cyberangriff die Praxisleitung dazu bewegen würde, ausreichende, finanzielle Ressourcen zur Verfügung zu stellen.

Obwohl oftmals die Praxisteams und BSI-Digitalen Ersthelfer wissen, was getan werden sollte, um die Sicherheit der Praxis zu gewährleisten, scheinen sie oft einfach nicht gehört zu werden. Ist das der Fall, kann sich unter den betroffenen Mitarbeitern ein gewisses Level an Frustration und Verärgerung aufbauen. Das Fatale daran sei, dass diese Mitarbeiter am Ende auch die Leidtragenden seien, wenn es zu einem Sicherheitsvorfall komme. Auf den '“ich habe es ja gesagt“-Moment folgten Angst und schlaflose Nächte. Als Mediator und IT-Spezialist hat Herr Peters oftmals nach dem Cyberangriff die Aufgabe, die Praxisleitung und das Praxisteam wieder zusammen zu führen. Leider gelingt das nicht immer und die Mitarbeiter/innen kündigen oder werden gekündigt.

Die Emotionskette nach dem Cyberangriff

Kommt es zu einer Cyberattacke, geht in der Regel alles sehr, sehr schnell: die Betroffenen Mitarbeiter werden - allen Vorbereitungen zum Trotz - meist von einem Emotionsmix heimgesucht. Auch wenn man sich auf eine solche Situation mit ITe@sy Notfallmanagement vorbereitet hat, neigt das Gehirn dazu, abzuschalten. Je intensiver die Cyber-Lage zu sein scheint, desto mehr neigt die Praxisleitung dazu, reaktiv und ohne nachzudenken zu handeln.
Die ersten Stunden nach einem Cyber-Sicherheitsvorfall sind dabei besonders panisch. Ich nenne das die "Panikphase"; wenn die blinde Panik einsetzt, fangen die Praxisteams an, Stromkabel herauszureißen, alles abzuschalten und die Internetverbindung zu kappen, weil sie nicht wissen, was sie tun sollen - außer einfach alles zum Stillstand zu bringen. Manche Mitarbeiter neigten in dieser Phase dazu, ihre Sorgen in körperliche Symptome umzuwandeln und dies habe ich schon selbst miterlebt. Ich kann mich an einen Ransomware-Angriff erinnern, wo der Arzt, mit dem ich telefonierte, die Backups gemeinsam mit seiner IT-Firma überprüfen und einspielen wollte. Nach einer Minute Ruhe hörte ich wie der IT´ler sich unter Tränen entschuldigen musste. Fast alle Backups waren nicht mehr zu verwenden und fast alle Daten weg. Sie hatten nichts mehr.

Überreaktionen und körperliche Symptome seien jedoch natürliche Reaktionen auf einschneidende Ereignisse. Das sind normale menschliche Reaktionen auf Stress. Es kann sehr niederschmetternd sein, wenn man feststellt, dass nicht nur ins Netzwerk eingedrungen wurde, sondern auch Daten gestohlen oder zerstört wurden – und zwar nicht nur die eigenen, sondern auch Kunden- oder Patientendaten.

Zu den Emotionen, die in den ersten Stunden nach einem Cyberangriff auftreten können, gehört auch Wut. Die richtet sich manchmal gegen den IT-Anbieter, der die Tools zur Verfügung gestellt hat, die den Angriff verhindern hätten sollen. Aber auch gegen die Cyberversicherung, die den Angriff nicht abwehren oder schlimmer noch nicht bezahlen möchte oder gegen die Angreifer, insbesondere wenn es sich beim Angriffsziel um eine Arzt- oder Zahnarztpraxis, einen Steuerberater/in oder Kleinunternehmen handelt. Schuldgefühle können in dieser Situation auftreten und diese oft im Zusammenhang mit Fahrlässigkeit. Dazu kommt es in der Regel, wenn erkannt wird, dass Warnzeichen übersehen wurden. Dennoch gibt es immer Apps oder Programme, die aktualisiert werden müssen.
Manche Mitarbeiter sind bessergestellt als andere Mitarbeiter, mit Stress dieser Art umzugehen. In diesen Fällen können Sicherheitsvorfälle langfristige Folgen für die psychische Gesundheit bedeuten. Glücklicherweise ist in der Cyberschutzbeauftragten-Weiterbildung von Praxismanagement Bublitz-Peters eine Selbstbewertung für die richtige Auswahl der Praxismitarbeiterin enthalten.

Taktisches Atmen

Als Experte für Krisenmanagement hat das Team von Praxismanagement Bublitz-Peters bereits umfassende Erfahrungen im Umgang mit brenzligen Situationen gesammelt. Eine Methode, die Cyber-Experten bei der Bewältigung geholfen hat, ist die „taktische Atmung“ (Combat Breathing). Sie wird unter anderem in Arztpraxen und Rettungsdiensten eingesetzt, um in gefährlichen Situationen Stress abzubauen. Bei der taktischen Atmung atmet man ein, während man bis vier zählt. Man hält den Atem an, während man bis vier zählt, atmet aus, während man bis vier zählt. Bei dieser Übung ist es wichtig, tief einzuatmen und dabei das Zwerchfell zu benutzen. In den angewendeten Arztpraxisnotfall-Schulungen von Praxismanagement Bublitz-Peters wird diese Übung schon lange angewendet.

Bei der aktiven Stressbewältigung können auch einfachere Techniken funktionieren, dazu gehören das verlängerte Ausatmen und die langsame Atmung. Verlängertes Ausatmen bedeutet, dass wir normal einatmen, aber langsam ausatmen. Langsames Atmen hingegen bedeutet, dass wir nur etwa sechs Zyklen des Ein- und Ausatmens pro Minute haben - im Gegensatz zur normalen Atemfrequenz. Wenn wir langsamer atmen, signalisieren wir unserem Körper, dass alles in Ordnung ist. Diese Übungen können unseren Herzschlag verlangsamen, unsere Muskeln entspannen und den Blutdruck senken.
Im Rahmen der ITe@sy-Notfallmanagement-Anwendung können diese Übungen ausgeführt werden.

Angriffstraining und -planung

Unabhängig von der Atemtechnik müssen Sie die Abläufe im Fall einer Cyberattacke so gut wie möglich vorab üben und im ITe@sy-Notfallplan beschreiben. Diese Übungen sollten idealerweise zusammen mit dem IT-Experten (oder IT-Firma) abgestimmt werden, denn alle Mitarbeiter/innen sollten an der praktischen Übung teilnehmen. Die Praxisleitung sollte mindestens einmal jährlich an einem Cyber-Workshop auf Grundlage der IT-Sicherheitsrichtlinie teilnehmen. Ich habe schon oft erlebt, dass die Praxisleitung nicht an einem solchen Training teilnehmen wollte, weil sie es als zu aufwendig empfanden oder einfach keinen Nutzen darin gesehen haben.

Grafik: Herr Mark Peters von Praxismanagement Bublitz-Peters bei einer Arztpraxisübung.

Um das zu verhindern, geht es im Cyber-Workshop von Praxismanagement Bublitz-Peters darum, die Leitung und Mitarbeiter im Umgang mit den Instrumenten zu schulen und nicht darum, IT-Managementpläne zu erstellen. Man sollte nie Mitarbeiter schulen, denen man nicht vorher die Antworten gibt. Bei den Kooperationsschulungen zwischen den KV´n, KZV´n, TÜV Süd, Ärztenetzen und Praxismanagement Bublitz-Peters stehen Fragen & Antworten (F&A) im Mittelpunkt
.
Übungen wie diese können sowohl Einzelpersonen als auch den Praxisteams dabei helfen, sicherer im Umgang von Cyber-Sicherheitsvorfällen zu werden. Im Anschluss sind sie dann in der Lage, bei Vorfällen besser zu reagieren und Emotionen effizienter zu filtern.

Die ITe@sy-Pläne für potenzielle Cyberangriffe haben sich als nützlich erweisen – es gibt einen ausgereiften Prozess, also einen dokumentierten Weg, mit einem Sicherheitsvorfall umzugehen. Somit ist es möglich, Emotionen auszuschalten, weil man nicht subjektiv handeln muss. Außerdem bin ich der Ansicht, dass Praxisteams davon profitieren könnten. Somit können Sie Karten neu mischen – eine Katastrophe kann in eine Chance verwandeln.
Damit diese Handlungsempfehlungen und Tipps funktionieren können, müssen auch die Praxisleitungen lernen, besser mit Cyber-Stress umzugehen.

Einfluss der Praxisleitung

Auch die Praxisleitung bzw. die Cyberschutzbeauftragten stehen bei einem Cybersecurity-Vorfall unter Druck: Ihr Unternehmen könnte Verluste einfahren und Reputationsschäden erleiden. Zudem müssen sich die Praxisteams unter Umständen mit verärgerten Kunden, Patienten oder Geschäftspartnern (Kliniken, Labore, Pflegeheime) auseinandersetzen, wenn dessen Daten vom Angriff betroffen sind.

Im Allgemeinen gibt es zwei Arten von Praxisleitungen: diejenigen, die in kritischen Zeiten wütend werden und Ihre Praxismitarbeiter/innen unter Druck setzen, um das Problem zu beheben und diejenigen, die Empathie und Mitgefühl zeigen. Sie sind bemüht, das Praxisteam bei der Einführung von Sicherheitsmaßnahmen zu unterstützen. Das Problem hierbei: die erstgenannte Gruppe verschlimmern die Situation. Solche Praxisleitungen müssen einen Schritt zurücktreten und verstehen, dass sie wahrscheinlich keinen hilfreichen Beitrag in dieser Lage leisten.

Praxismanagement
Bublitz-Peters GmbH & Co. KG
Rohrbacher Str. 28
69115 Heidelberg

Sitz: Heidelberg
Geschäftsführerin: Silke Bublitz-Peters
Registernummer: HRA 701358
Amtsgericht: Mannheim

Telefon: +49 (0)6221-43 85 00
Telefax: +49 (0)6221-43 85 01 10
Mail: praxischeck@bublitz-peters.de
www.bublitzpeters.de

Zu Ergänzen ist, dass auch BSI-Digitale Ersthelfer gerne Dinge übersehen könnten, wir BSI- in Eile handeln müssen – denn bei Druck, werden oft Fehler gemacht.
Sicherheitsexperten neigen dazu, sich mehr auf die Wiederherstellung als auf die Forensik zu konzentrieren. Sie müssen nachvollziehen, wie es zu dem Angriff gekommen ist - nicht nur, damit Sie Ihr Sicherheitsniveau in Zukunft verbessern können, sondern auch, um sicherzustellen, dass die Angreifer nicht mehr im Netzwerk sind.
Im Gegensatz dazu kann eine unterstützende Praxisleitung dazu beitragen, die Praxiskrise schneller aufzulösen. Ich empfehle den Cyberschutzbeauftragten ihr Team zu fragen, wie sie unterstützen können. Es ist wichtig, dass die Führungsebene diese Art von Teamarbeit an den Tag legt. Emotionen können Menschen herunterziehen, aber sie können sie auch aufrichten und motivieren. Es geht darum, das System und die Menschen so zu führen, dass wir immer einen positiven Antrieb haben und nicht auf die Bremse treten.
Die kritische Phase eines Sicherheitsvorfalls ist nicht die Zeit für „Schuldzuweisungen", sondern die Zeit für echte Teamarbeit.

High Level-Beruhigung

In den extremen Momenten einer Datenschutzverletzung verbringe ich einen Großteil meiner Zeit damit, nervöse Praxisleitungen zu beruhigen. Wir sind bis zu einem gewissen Grad die *starke Schulter* und helfen dabei, mit den aufkommenden Gefühlen umzugehen. Als Praxismediator habe ich Erfahrungen, mit extremen Situationen umzugehen. Jeder Mensch nimmt Informationen auf unterschiedliche Weise auf. Manche Menschen sind sehr praktisch veranlagt, andere bevorzugen schriftliche Reportings. Viel Zeit für Gespräche bedeutet allerdings auch, dass weniger an der Behebung des Problems gearbeitet wird.

Oft verlassen ich mit den Cyberschutzbeauftragten oder der Praxisleitung den Besprechungsraum und führe eine Anti-Stress-Nachbesprechung durch. Hierbei erkläre ich wie man die Dinge wieder in den Griff bekommen kann und kann auch telefonisch erfolgen. In diesem Rahmen moderiere ich als externer Koordinator die Lösung des Cyberprozesses zwischen der Praxis, der IT-Firma, der Datenschutzbehörde und der Polizei (ZAC).

In gefährlichen Situationen ist es von entscheidender Bedeutung, dass alle Beteiligten Ruhe bewahren. Wir können noch so viele Hilfsmittel einsetzen, doch wenn die betreffende Person nicht über die nötige Belastbarkeit verfügt, wird es trotzdem schwierig, die gewünschten Ergebnisse zu erzielen.

Quelle: Praxismanagement Bublitz-Peters, BSI, TÜV Süd

Hier erhalten Sie mehr Informationen zur *Motivierten Cyberschutzarbeit*.

SCAN ME

Praxismanagement
Bublitz-Peters GmbH & Co. KG
Rohrbacher Str. 28
69115 Heidelberg

Sitz: Heidelberg
Geschäftsführerin: Silke Bublitz-Peters
Registernummer: HRA 701358
Amtsgericht: Mannheim

Telefon: +49 (0)6221-43 85 00
Telefax: +49 (0)6221-43 85 01 10
Mail: praxischeck@bublitz-peters.de
www.bublitzpeters.de